RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2018

Section Contracts and Grants with Industry

Edition: 2019-03-07

Algorithmics, Computer Algebra and Cryptology

Architecture, Languages and Compilation

Embedded and Real-time Systems

Proofs and Verification

SECURITY AND CONFIDENTIALITY

ARIC Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Bosch (Germany) ordered from us some support for implementing complex numerical algorithms (participants: Claude-Pierre Jeannerod and Jean-Michel Muller).

8.2. Bilateral Grants with Industry

- Miruna Rosca and Radu Titiu are employees of BitDefender. Their PhD's are supervised by Damien Stehlé and Benoît Libert, respectively. Miruna Rosca works on the foundations of lattice-based cryptography, and Radu Titiu works on pseudo-random functions and functional encryption.
- Adel Hamdi is doing is PhD with Orange Labs and is supervised by Fabien Laguillaumie. He is working on advanced encryption protocols for the cloud.

AROMATH Project-Team (section vide)

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- We have training and consulting activities with the French Ministry of Defense.
- Together with the PESTO team, we have a contract with the Docapost company, the purpose of which is to impove their e-voting solution by adding some verifiability properties and switching to elliptic curve cryptography.
- In this contract handled in collaboration with the University of Bristol and the PESTO team, the goal is to audit and prove security properties of a new e-voting protocol called CHVote, to be used in a few cantons of Switzerland.

8.2. Bilateral Grants with Industry

- This contract with Orange Gardens at Chatillon-Montrouge is dedicated to the supervision of Sandra Rasoamiaramanana's PhD thesis about security in the white box context. The co-supervisor for Orange Gardens is Gilles Macario-rat.
- This contract with Thales (Thales Communication & Security, Genneviliers, subsidiary of Thales Group) is dedicated to the supervision of Simon Masson's PhD thesis about elliptic curves for bilinear and post-quantum cryptography. The co-supervisor for Thales is Olivier Bernard.

CASCADE Project-Team (section vide)

DATASHAPE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- Collaboration with Sysnav, a French SME with world leading expertise in navigation and geopositioning in extreme environments, on TDA, geometric approaches and machine learning for the analysis of movements of pedestrians and patients equipped with inetial sensors (CIFRE PhD of Bertrand Beaufils).
- Research collaboration with Fujitsu on the development of new TDA methods and tools for Machine learning and Artificial Intelligence (started in Dec 2017).

8.2. Bilateral Grants with Industry

- DATASHAPE and Sysnav have been selected for the ANR/DGA Challenge MALIN (funding: 700 kEuros) on pedestrian motion reconstruction in severe environments (without GPS access).

GAIA Team

8. Bilateral Contracts and Grants with Industry

8.1. Safran Electronics & Defense

Within the CIFRE PhD thesis (2014-2018) [15], we have studied new robust stabilization techniques for gyrostabilized systems with unfixed model parameters (e.g. modes, masses, stiffness of springs, damper magnitudes). Parameters of their models indeed slowly change with the temperature, fatigue, etc., yielding time-consuming re-computations of robust controllers. Moreover, the possibility to quickly know robustness indicators (e.g. margins) and explicit robust controllers in terms of the model parameters can highly speed up the design of a project. Finally, closed-form solutions for robust controllers in terms of the model parameters are the first steps towards the development of adaptive robust controllers which can be embedded in gyrostabilized platforms since no optimization algorithms are then required for a real-time implementation and only the parameters have to be estimated from time to time to re-compute the robust controller (based on a basic arithmetic). To do that, we have introduced algebraic methods and computer algebra techniques to initiate a new approach entitled *parametric robust control*. For mor details, see [15] and [98], [100], [99]. This new approach will be further developed in the future since it opens both theoretical and practical interesting questions. In particular, the new PhD thesis of Grace in GAIA aims to study the underlying mathematical problem from both a theoretical and an implementation perspectives.

8.2. Ellcie Healthy

A new collaboration with Ellcie Healthy, a company based in Nice began in October 2017. It involves the analyze of signals coming from optical sensors installed in glasses. With Denis Efimov, the first studies obtained were very promising. This collaboration was formalized with the signature of a first contract in March 2018. The first objective of this project was to design algorithms for intelligent filtering of data coming from infrared sensors, especially for light-related disturbances. Discussions are currently underway for the submission of new joint projects.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- Company: WATERLOO MAPLE INC
  Duration: 2 years
  Participants: GAMBLE and OURAGAN Inria teams
  Abstract: A two-years licence and cooperation agreement was signed on April 1st, 2018 between WATERLOO MAPLE INC., Ontario, Canada (represented by Laurent Bernardin, its Executive Vice President Products and Solutions) and Inria. On the Inria side, this contract involves the teams GAMBLE and OURAGAN (Paris), and it is coordinated by Fabrice Rouillier (OURAGAN).

  F. Rouillier and GAMBLE are the developers of the ISOTOP software for the computation of topology of curves. One objective of the contract is to transfer a version of ISOTOP to WATERLOO MAPLE INC.
- Company: GEOMETRYFACTORY
  Duration: permanent
  Participants: Inria and GEOMETRYFACTORY
  Abstract: CGAL packages developed in GAMBLE are commercialized by GEOMETRYFACTORY.

GRACE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Nokia

Participants: Daniel Augot, Nicholas Coxon, Françoise Levy-Dit-Vehel.

Phase 2 has been finished, while a new phase, phase 3, has been negociated between Inria and Nokia. Grace finished his work on fast algorithms for polynomials over fields of small caracteristic, wth application to coding theory, multiplicity codes and private information retrieval. The new phase will fund a project on rank-metric codes for security and privacy in cloud storage (in collaboration with Gilles Zémor, Uni. Bordeaux).

LFANT Project-Team (section vide)

OURAGAN Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

The objective of our Agrement with WATERLOO MAPLE INC. is to promote software developments to which we actively contribute.

On the one hand, WMI provides man power, software licenses, technical support (development, documentation and testing) for an inclusion of our developments in their commercial products. On the other hand, OURAGAN offers perpetual licenses for the use of the concerned source code.

As past results of this agreement one can cite our C-Library *RS* for the computations of the real solutions zero-dimensional systems or also our collaborative development around the Maple package *DV* for solving parametric systems of equations.

For this term, the agreement covers algorithms developed in areas including but not limited to: 1) solving of systems of polynomial equations, 2) validated numerical polynomial root finding, 3) computational geometry, 4) curves and surfaces topology, 5) parametric algebraic systems, 6) cylindrical algebraic decompositions, 7) robotics applications.

In particular, it covers our collaborative work with some of our partners, especially the Gamble Project-Team - Inria Nancy Grand Est.

POLSYS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

Until the mid 2000's, multivariate cryptography was developing very rapidly, producing many interesting and versatile public-key schemes. However, many of them were soon successfully cryptanalysed (a lot have been done in this group). As a consequence, the confidence in multivariate cryptography cryptosystems declined. It seems that there have emerged new important reasons for renewal of the interest in a new generation of multivariate schemes. In the past two years, the algorithms for solving the Discrete Logarithm Problem over small characteristic fields underwent an extraordinary development. This clearly illustrates the risk to not consider alternatives to classical assumptions based on number theory. In parallel, two of the most important standardization bodies in the world, NIST and ETSI have recently started initiatives for developing cryptographic standards not based on number theory, with a particular focus on primitives resistant to quantum algorithms. An objective here is then to focus on the design of multivariate schemes.

The team is involved in the industrial transfer of post-quantum cryptography. The maturation project, called HFEBoost, is supervised by SATT-LUTECH.

SATT-LUTECH specializes in the processing and transfer of technologies from research laboratories of its shareholders: Inria, CNRS, University of Technology of Compiègne National Museum of Natural History, Institute Curie, Université Panthéon-Assas, Paris Sorbonne University and National School of Industrial Creation).

The team has recently developed, in partnership with a mobile application development company (WASSA), an Android app for smartphones (Samsung S5 type) that uses multivariate cryptography. The application has been tested mid-November in a series of experiments supervised by DGA and French Ministry of Defense. The experiment gathered a total of hundred participants from various operational units. This is a first milestone in the maturation project whose goal is to create a start-up.

7.2. Public Contracts

CEA LETI / DSYS / CESTI

In smart card domain, the emanations of a component during a cryptographic computation may compromise the information that is directly or not linked to the secret keys. The most part of the side channel attacks are based on statistical tools that exploit relations between the handled data and the signals. However these methods do not take advantage of all the signal information. The goal is to study the existing algorithms in pattern and speech recognition and to apply them to signals related to cryptographic computations. The objective will be to improve the attacks efficiency and resolve more complex problems.

- CIFRE Contract with ST Micro electronics that funds the PhD thesis of Simon Landry on "Threshold Implementations Against Side Channel Analysis". Supervisor Emmanuel Prouff.

SECRET Project-Team (section vide)

SPECFUN Project-Team (section vide)

CAIRN Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Collaboration with Huawei Technologies, Sophia Antipolis: In the context of Image Signal Processing (ISP), the project aims at building a proof of concept of an environment able to automatically optimize the precision of every operator (fixed-point or floating-point arithmetic) in a complex, multi-kernel algorithm and find the best tradeoff between cost/power and image quality.

CAMUS Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Caldera

Vincent Loechner and Cédric Bastoul are involved in a collaboration with the Caldera company (http://www.caldera.com), specialized in software development for wide image processing. The goal of this collaboration is the development of parallel and scalable image processing pipeline for industrial printing. The project started in September 2016 and involves a contract established between the ICube laboratory and the Caldera company. It also includes the funding of the industrial thesis (CIFRE) of Paul Godard (started in September 2016) on the topic of the collaboration, under the supervision of Vincent Loechner and Cédric Bastoul.

CASH Team (section vide)

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- CORSE is involved in a contract with Atos/Bull which objective is the objective is to optimize the energy consumption of HPC applications on large scale plateforms.

8.2. Bilateral Grants with Industry

- ES3CAP is a bilateral grant with Kalray. CORSE is involved in the optimisation of machine learning algorithms for many-core architectures.

PACAP Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Intel research grant INTEL2016-11174

Participants: Niloofar Charmchi, Kleovoulos Kalaitzidis, Pierre Michaud, André Seznec.

Intel is supporting the research of the PACAP project-team on “Design tradeoffs for extreme cores”.

AOSTE2 Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

The IFPEN grant which started on December 2014 and ended on February 2018, provides full support for the PhD thesis of Salah Eddine Saidi. The thesis concerns the automatic parallelization and scheduling approaches for co-simulation of numerical models on multi-core processors. The goal of the first research topic is to propose multi-core scheduling solutions for the co-simulation in order to accelerate its execution. The second research topic aims at proposing multi-core scheduling solutions in order to enable the execution of co-simulation under real-time constraints in the context of Hardware-in-the-Loop validation.

HYCOMES Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Glose: Globalisation for Systems Engineering

Participants: Benoît Caillaud, Benoît Vernay.

Glose is a bilateral collaboration between Inria and Safran Tech., the corporate research entity of Safran Group. It started late 2017 for a duration of 44 months. Three Inria teams are involved in this collaboration: Diverse (Inria Rennes), Hycomes and Kairos (Inria Sophia-Antipolis). The scope of the collaboration is systems engineering and co-simulation.

The simulation of system-level models requires synchronizing, at simulation-time, physical models with software models. These models are developed and maintained by different stakeholders: physics engineers, control engineers and software engineers. Models designed by physics engineers are either detailed 3D finite-elements models, with partial differential equations (PDEs), or finite-dimension 0D models (obtained by model reduction techniques, or by empirical knowledge) expressed in modeling languages such as Simulink (with ordinary differential equations, or ODEs), Modelica (with differential algebraic equations, or DAEs), or directly as a C code embedding both the differential equations and its discretization scheme. Coupling together heterogeneous models and programs, so that they can be co-simulated, is not only a technological challenge, but more importantly raises several deep and difficult questions: Can we trust simulations? What about their reproducibility? Will it be possible to simulate large systems with hundreds to thousands of component models?

Co-simulation requires that models are provided with interfaces, specifying static and dynamic properties about the model and its expected environments. Interfaces are required to define how each model may synchronize and communicate, and how the model should be used. For instance, an interface should define (i) which variables are inputs, which are outputs, (ii) their data types, physical units, and sampling periods, but also (iii) the environmental assumptions under which the model is valid, and (iv) the causal dependencies between input and output variables and for continuous-time models, (v) the stiffness of the model, often expressed as a time-varying Jacobian matrix.

Formally, an interface is an abstraction of a model's behavior. A typical example of interface formalism for 0D continuous-time models is the FMI standard. Co-simulation also requires that a model of the system architecture is provided. This architectural model specifies how components are interconnected, how they communicate and how computations are scheduled. This is not limited to the topology of the architecture, and should also specify how components interact. For instance, variables in continuous-time models may have different data-types and physical units. Conversion may be required when continuous-time models are plugged together. Another fine example is the coupling of a 3D finite-element model to a 0D model: effort and flow fields computed in the 3D model must be averaged in a scalar value, before it can be sent to the 0D model, and conversely, scalar values computed by the 0D model must be distributed as a (vector) field along a boundary manifold of the 3D model. For discrete-time models (eg., software), components may communicate in many ways (shared variables, message passing, ...), and computations can be time- or event-triggered. All these features are captured as data-/behavior-coordination patterns, as exemplified by the GEMOC initiative [0].

[0] http://gemoc.org

In the Glose project, we propose to formalize the behavioral semantics of several modeling languages used at system-level. These semantics will be used to extract behavioral language interfaces supporting the definition of coordination patterns. These patterns, in turn, can systematically be used to drive the coordination of any model conforming to these languages. The co-simulation of a system-level architecture consists in an orchestration of hundreds to thousands of components. This orchestration is achieved by a master algorithm, in charge of triggering the communication and computation steps of each component. It takes into account the components' interfaces, and the data-/behavior-coordination patterns found in the system architecture model. Because simulation scalability is a major issue, the scheduling policy computed by the master algorithm should be optimal. Parallel or distributed simulations may even be required. This implies that the master algorithm should be hierarchical and possibly distributed.

KAIROS Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Safran: Desir/Glose

Participants: Julien Deantoni, Giovanni Liboni, Robert de Simone.

We participate to the bilateral collaborative program Desir, put up by Safran to work with selected academic partners. We share the Glose project started in this program with HyComes, and DiverSE Inria project teams. Technically, the goal of this project is to elaborate on the (under development) Safran's system engineering method to make it simulable at different steps of the development, possibly early in the design process and possibly mixing models at different maturity level. This project is strongly connected to results depicted in Section 7.6 .

8.1.2. IRT Saint-Exupery ATIPPIC

Participants: Paul Bouche, Amin Oueslati, Robert de Simone, Julien Deantoni.

In an attempt to build an extension of IRT Saint-Exupery from Occitanie to PACA region, the Thales Alenia Space company promoted the ATIPPIC project, to build the computing digital electronic structure of micro-satellites on ordinary, "COTS" processors. The project was accepted for 30 months, funds two temporary research engineers working under our own supervision, while exchanging extensively with the rest of the ATIPPIC project, which is actually hosted by Inria. The technical content of our contributions is described in Section 7.5 and 7.7 .

8.1.3. Renault Software Lab

Participants: Frédéric Mallet, Marie-Agnès Peraldi-Frati, Robert de Simone.

We have just started, at the end of 2018, a collaboration with Renault Software Labs on the definition of rules for ensuring safe maneuvers in autonomous vehicles. The rules express conditions from the environments, safety rules to preserve the integrity of the vehicles, driving legislation rules, local rules from the authorities. The rules must be updated dynamically when the vehicle evolves and are used to monitor at run-time the behavior of the ADAS. While the ADAS contains several algorithms relying on machine learning, the monitoring system must be predictive and rules must guarantee formally that the system does not cause any accident. So it can be seen as a way to build trustworthy monitoring of learning algorithms. A CIFRE PhD will start at the beginning of 2019.

8.1.4. Accenture Labs, Sophia

Participant: Luigi Liquori.

We started in 2018 a collaboration with Accenture Labs, Sophia on the following topics:

- Smart Contract languages for permissioned blockchains. We saw in the recent years the development of different platforms that focuses on the so-called private (or permissioned) blockchain(s) and digital ledgers. Almost the totality of private blockchain(s) present their own implementation of Smart Contract. Between public and private blockchains we are observing a wide variety of different languages with different capabilities and limitations. Both public and private blockchain often lack maturity and a formal semantic as they have been under pressure of the sudden and rapid explosion of blockchain popularity. A CIFRE PhD will start in 2019.
- Oracles in Smart Contract for IoT and and CPS. Oracles are third party services which are not part of the blockchain consensus mechanism. The main challenge with oracles is that people need to trust these sources of information. Whether a website or a sensor, the source of information needs to be trustworthy. The main challenges for oracles are dealing with small computation power, mobility, security and dealing with time. A CIFRE PhD is planned to start in 2019.

PARKAS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Polly Labs contract with ARM, 2015-2019, with the participation of Qualcomm, Xilinx and Facebook (human resources, consulting services and and hiring former PARKAS members).

7.2. Bilateral Grants with Industry

In 2018 Francesco Zappa Nardelli was awarded a Google Research Fellowship to pursue the work on DWARF unwinding, about 50k euros.

SPADES Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- Inria and Orange Labs have established in 2015 a joint virtual research laboratory, called I/O LAB. We have been heavily involved in the creation of the laboratory and are actively involved in its operation (Jean-Bernard Stefani is one of the two co-directors of the lab). I/O LAB focuses on the network virtualization and cloudification. As part of the work of I/O LAB, we have cooperated with Orange Lab, as part of a cooperative research contract funded by Orange, on defining architectural principles and frameworks for network cloud infrastructures encompassing control and management of computing, storage and network resources.
- With Daimler (subcontracting via iUTBS): We have proposed, in collaboration with TU Braunschweig, an extension of the LET paradigm [50], called *System-level LET, to accommodate the specific needs of the design process in the automotive industry, in which the network structure must be made explicit in the LET program.*

7.2. Bilateral Grants with Industry

With Thales: Early performance assessment for evolving and variable cyber-physical systems. This CIFRE grant funds the PhD of Christophe Prévot.

With Orange: Programming IoT and sofware defined radio with dynamic dataflow models of computation. This CIFRE grant funds the PhD of Arash Shafiei.

TEA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Inria – Mitsubishi Electric framework program (2018+)

Title:

Inria principal investigator: Jean-Pierre Talpin, Simon Lunel

International Partner: Mitsubishi Electric R&D Europe (MERCE)

Duration: 2018

Abstract: Following up the fruitfull collaboration of TEA with the formal methods group at MERCE, Inria and Mitsubishi Electric signed a center-wide collaboration agreement, which currently hosts projects with project-teams Sumo and Tea.

8.1.2. Mitsubishi Electric R&D Europe (2015-2018)

Title: Analysis and verification for correct by construction orchestration in automated factories

Inria principal investigator: Jean-Pierre Talpin, Simon Lunel

International Partner: Mitsubishi Electric R&D Europe

Duration: 2015 - 2018

Abstract: The primary goal of our project is to ensure correctness-by-design in cyber-physical systems, i.e., systems that mix software and hardware in a physical environment, e.g., Mitsubishi factory automation lines. We develop a component-based approach in Differential Dynamic Logic allowing to reason about a wide variety of heterogeneous cyber-physical systems. Our work provides tools and methodology to design and prove a system modularly.

ANTIQUE Project-Team (section vide)

CELTIQUE Project-Team (section vide)

CONVECS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

7.1.1. Orange Labs

Participants: Umar Ozeer, Gwen Salaün.

Umar Ozeer is supported by a PhD grant (from November 2016 to November 2019) from Orange Labs (Grenoble) on detecting and repairing failures of data-centric applications distributed in the cloud and the IoT (see § 6.5.1), under the supervision of Loïc Letondeur (Orange Labs), Gwen Salaün (CONVECS), François Gaël Ottogalli (Orange Labs), and Jean-Marc Vincent (POLARIS project-team).

7.1.2. Nokia Bell Labs

Participants: Radu Mateescu, Ajay Muroor Nadumane, Gwen Salaün.

Ajay Muroor Nadumane is supported by a PhD grant (from October 2017 to October 2020) from Nokia Bell Labs (Nozay) on IoT service composition supported by formal methods, under the supervision of Gwen Salaün (CONVECS), Radu Mateescu (CONVECS), Ludovic Noirie, and Michel Le Pallec (Nokia Bell Labs).

DEDUCTEAM Project-Team (section vide)

GALLINETTE Project-Team (section vide)

GALLIUM Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. The Caml Consortium

Participants: Damien Doligez [**contact**], Xavier Leroy, Michel Mauny, Didier Rémy.

The Caml Consortium is a formal structure where industrial and academic users of OCaml can support the development of the language and associated tools, express their specific needs, and contribute to the long-term stability of OCaml. Membership fees are used to fund specific developments targeted towards industrial users. Members of the Consortium automatically benefit from very liberal licensing conditions on the OCaml system, allowing for instance the OCaml compiler to be embedded within proprietary applications.

The Consortium currently has 15 member companies:

- Aesthetic Integration
- Ahrefs
- Be Sport
- Bloomberg
- CEA
- Citrix
- Docker
- Esterel Technologies
- Facebook
- Jane Street
- Kernelyze LLC
- LexiFi
- Microsoft
- OCamlPro
- SimCorp

For a complete description of this structure, please refer to https://ocaml.org/consortium/index.html.

The Caml Consortium is being gradually phased out. In the future, it should be entirely replaced by the OCaml Foundation, described next (§8.1.2).

8.1.2. The OCaml Foundation

Participant: Michel Mauny.

In June 2018, Michel Mauny created the OCaml Software Foundation (OCSF), a structure sheltered by the Inria Foundation. The OCSF now has a few patrons. With the help of Yann Régis-Gianas, it is running the Learn-OCaml project, which aims at developing the usage of OCaml in higher education. A paper that presents the project has been accepted for publication at JFLA 2019 [20]. The OCaml Software Foundation and the Learn-OCaml project have been presented at the 2018 OCaml workshop.

The OCaml Software Foundation is expecting more patrons at the beginning of 2019, and shall organize meetings where donors discuss and produce suggestions for actions of general interest to be funded.

MARELLE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Together with IMDEA Madrid (Spain), INESC TEC (Portugal), the Catholic University of Louvain (Belgium), Google, and Ecole Polytechnique, with have a contract with Amazon Web Services. The financial return for Marelle is 67kEuros.

MEXICO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Our cooperation with industry took place in the context of a multi-lateral SystemX project, see below.

MOCQUA Team (section vide)

PARSIFAL Project-Team (section vide)

PI.R2 Project-Team (section vide)

SUMO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Nokia Bell Labs - ADR SAPIENS

Several researchers of SUMO are involved in the joint research lab of Nokia Bell Labs France and Inria. We participate in the common research team SAPIENS (Smart Automated and Programmable Infrastructures for End-to-end Networks and Services), previously named “Softwarization of Everything.” This team involves several other Inria teams : Convecs, Diverse and Spades. SUMO focuses on the management of reconfigurable systems, both at the edge (IoT based applications) and in the core (e.g. virtualized IMS systems). In particular, we focus on control and diagnosis issues for such systems. Two PhD students are involved in the project. Erij Elmajed (2nd year), on the topic of Diagnosis of virtualized and reconfigurable systems supervised by Éric Fabre and Armen Aghasaryan (Nokia Bell Labs). Abdul Majith (to start in January 2019) on Controller Synthesis of Adaptive Systems, supervised by Hervé Marchand, Ocan Sankur, and Dinh Thai Bui (Nokia Bell Labs).

8.1.2. Orange Labs

SUMO is participating in IOLab, the common lab of Orange Labs and Inria, dedicated to the design and management of Software Defined Networks. Our activities concern the diagnosis of malfunctions in virtualized multi-tenant networks. This collaboration supports one Cifre PhD student, Sihem Cherrared (2nd year), supervised by Eric Fabre, Gregor Goessler (Inria team Spades in Grenoble) and Sofiane Imadali (Orange Labs).

8.1.3. Alstom Transport - P22

Joint Alstom-Inria research lab: Several researchers of SUMO are involved in the joint research lab of Alstom and Inria, in a common research team called P22. On Alstom side, this joint research team involves researchers of the ATS division (Automatic Train Supervision). The objective of this joint team is to evaluate regulation policies of urban train systems, to assess their robustness to perturbations and failures, to design more efficient regulation policies and finally to provide decision support for human regulators. The project started in march 2014. A second phase of the project started in 2016, for a duration of three years. This covers in particular the CIFRE PhD of Karim Kecir.

8.1.4. Mitsubishi Electric Research Center Europe (MERCE)

Several researchers of SUMO are involved in a collaboration with the formal verification team of MERCE on model checking of real-time systems. The members of the formal verification team at MERCE work on different aspects of formal verification and participate to academic collaborations.

The SUMO team and MERCE have jointly supervised an M1 internship (Ludovic Landuré), and are supervising a Cifre PhD student (Emily Clement) funded by MERCE, started this fall. Reiya Noguchi, a member of MERCE will be hosted by the SUMO team in 2019.

TOCCATA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. ProofInUse Joint Laboratory

Participants: Claude Marché [contact], Jean-Christophe Filliâtre, Andrei Paskevich, Guillaume Melquiond, Sylvain Dailler.

The objective of ProofInUse is to provide verification tools, based on mathematical proof, to industry users. These tools are aimed at replacing or complementing the existing test activities, whilst reducing costs.

This laboratory is a joint effort of the Inria project-team Toccata, the AdaCore company which provides development tools for the Ada programming language, and the TrustInSoft company which provides static analysis tools for the C and C++ programming language.

The objective of ProofInUse is thus to significantly increase the capabilities and performances of verification environments proposed by these two companies. It aims at integration of verification techniques at the state-of-the-art of academic research, via the generic environment Why3 for deductive program verification developed by Toccata.

This joint laboratory is a follow-up of the former "LabCom ProofInUse" between Toccata and AdaCore, funded by the ANR programme "Laboratoires communs", from April 2014 to March 2017 http://www.spark-2014.org/proofinuse.

The SME AdaCore is a software publisher specializing in providing software development tools for critical systems. A previous successful collaboration between Toccata and AdaCore enabled *Why3* technology to be put into the heart of the AdaCore-developed SPARK technology.

The SME TrustInSoft is a company whose speciality is the verification of critical software, written in the C or C++ languages. It is interested in integrating the novelties of ProofInUse in its own environment TIS Analyzer.

8.2. Bilateral Grants with Industry

8.2.1. CIFRE contract with TrustInSoft company

Participants: Guillaume Melquiond [contact], Raphaël Rieu-Helft.

Jointly with the thesis of R. Rieu-Helft, supervised in collaboration with the TrustInSoft company, we established a 3-year bilateral collaboration contract, that started in October 2017. The aim is to design methods that make it possible to design an arbitrary-precision integer library that, while competitive with the state-of-the-art library GMP, is formally verified. Not only are GMP's algorithm especially intricate from an arithmetic point of view, but numerous tricks were also used to optimize them. We are using the Why3 programming language to implement the algorithms, we are developing reflection-based procedures to verify them, and we finally extract them as a C library that is binary-compatible with GMP [20] [26].

VERIDIS Project-Team (section vide)

CIDRE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **HP (2013-2019): Embedded Systems Security** We aim at researching and prototyping low-level intrusion detection mechanisms in embedded system software. This involves mechanisms in continuation of previous work realized by our team as well as investigating new techniques more directly tied to specific HP device architectures. Our main objective is to monitor low-level software (firmware, OS kernels, hypervisors) thanks to a dedicated external co-processor. Ronny Chevalier is doing is PhD in the context of this project. Being under NDA, details about this research program cannot be provided.

7.2. Bilateral Grants with Industry

- **ANSSI: Security of Low-level Components** Thomas Letan has started his PhD thesis in the context of a contract between CentraleSupelec and the French National Computer Security Agency (ANSSI). His work consists in using formal methods to specify hardware/software security mechanisms and to verify that they correctly enforce some security policies.
- **DGA: Visualization for security events monitoring** Damien Crémilleux has started his PhD thesis in October 2015 in the context of a cooperation with DGA-MI. The subject of the PhD is to define relevant representations to allow front-line security operators to monitors systems from a security perspective. A first proposal was made that led to a tool, VEGAS, that allows to monitor large quantities of alerts in real time and to dispatch these alerts in a relevant way to security analysts.
- **DGA: Intrusion Detection in Distributed Applications** David Lanoé has started his PhD thesis in October 2016 in the context of a cooperation with DGA-MI. His work is focussing on the construction of behavioral models (during a learning phase) and their use to detect intrusions during an execution of the modelled distributed application.
- **DGA: Protection against fuzzing attack** Aurelien Palisse has started his PhD in October 2015 in the context of a cooperation with DGA-MI. The subject of the PhD is to propose a detection mechanism and a mitigation procedure to counter ransomware attacks. He designed a low cost Windows driver that use a Markov chain as a model for an anomaly detection system. The technology has been patented by both Inria and DGA.
- **Idemia: Hardware Security for Embeded Devices** Kevin Bukasa has started his PhD in January 2016 in a bilateral contract between Inria and Idemia. He explored fault injection attacks using EM probes on two different kind of devices: microcontroller (representing IoT) and SoC (representing Smart phone). He demonstrated the vulnerability of both architectures on this kind of attack. On IoT device he has developped an attack allowing to take a full control on the device. He discovered also new fault attacks never described in the litterature.
- **Idemia: Protection against fuzzing attack** Leopold Ouairy has started his PhD in October 2017 in a bilateral contract between Inria and Idemia. The context is related with security testing of Java applications to avoid fuzzing attack. The approach is based on AI to design automatically a model use for the oracle. He used machine learning to serach in a corpus of applicatons methods having the same semantics. Then in a second step, after convertir the source code into a vector he compute a similarity value which is related with absence of conditions evaluation.

- **Ministry of Defence: Visualisation for the characterization of security events** Laetitia Leichtnam has started his PhD thesis in November 2016 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work consists in presenting events appearing in heterogeneous logs as a dependency graph between the lines of logs. This permits to the administrator to investigate easily the logs to discover the different steps that has performed an attack in the supervised system.
- **Ministry of Defence: Characterization of an attacker** Aïmad Berady has started his PhD thesis in November 2018 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work is to highlight the characteristics of an attacker performing a targeted and long-term attack on an information system.
- **Nokia: Risk-aware security policies adaptation in modern communication infrastructures** Pernelle Mensah was hired in January 2016 on this CIFRE funding in order to work on unexplored aspects of information security, and in particular response strategies to complex attacks, in the context of cloud computing architectures. The use case proposed by our industrial partner is a multi-tenant cloud computing platform involving software-defined networking in order to provide further flexibility and responsiveness in architecture management. The topic of the thesis is to adapt and improve the current risk-aware reactive response tools, based on attack graphs and adaptive security policies, to this specific environment, taking into account the heterogeneity of actors, platforms, policies and remediation options.
- **Orange LAb's: Storage and query in a massive distributed graph for the web of things** Cyprien Gottstein has started his PhD thesis in October 2018 in the context of a collaboration between Inria and Orange (I/O Lab). In this thesis, we consider storage and query problems that arise when massive distributed graphs are used to represent the web of things. In particular, access to the data and partitioning of the graph are studied to propose efficient geographical services.
- **Thales: Privacy and Secure Multi-party Computation** Aurélien Dupin has started his PhD thesis in January 2016 within the context of a CIFRE contract with Thales. His PhD subject concerns secure multi-party computation. Secure two-party computation provides a way for two parties to compute a function, that depends on the two parties' inputs, while keeping them private. Known since the 1980s, Yao's garbled circuits appear to be a general solution to this problem, in the semi-honest model. Decades of optimizations have made this tool a very practical solution. However, it is well known that a malicious adversary could modify a garbled circuit before submitting it. Many protocols, mostly based on cut-&-choose, have been proposed to secure Yao's garbled circuits in the presence of malicious adversaries. Nevertheless, how much an adversary can modify a circuit and make it still executable have not been studied. In the context of his PhD, Aurélien Dupin is interested by such a question.
- **Thales: Combining Attack Specification and Dynamic Learning from traces for correlation rule generation** Charles Xosanavongsa has started his PhD thesis in December 2016 in the context of a CIFRE with Thales. His work will focus on the construction of correlation rules. In previous work on correlation rule generation, the usual approach is static. It always relies on the description of the supervised system using a knowledge base of the system. The use of correlation trees is an appealing solution because it allows to have a precise description of the attacks and can handle any kind of IDS. But in practice, the behavior of each IDS is quite difficult to predict, in particular for anomaly based IDS. To manage automatically the correlation rules (and adapt them if necessary), we plan to analyze synthetic traces containing both anomaly based and misused based IDS alerts resulting from an attack.

COMETE Project-Team (section vide)

DATASPHERE Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

The PhD Thesis of Colin Gerard is funded through a contract with DGA (Ministry of Defense).

PESTO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

We have several contracts with industrial partners interested in the design of electronic voting systems:

- Since 2014, a collaboration agreement has been signed between Pesto and Scytl, a Spanish company which proposes solutions for the organization of on-line elections, including legally binding elections, in several countries. In this context, a first contract has been signed in 2016 to design a formal proof of both verifiability and privacy of the protocol developed by Scytl, for a deployment in Switzerland. In 2018, a new contract has been signed to adapt the previous security proof to the new protocol proposed by Scytl, in order to achieve universal verifiability.
- The canton of Geneva signed a contract in October 2017 with Pesto and Caramba, as well as Manifold Security (Bogdan Warinschi and David Bernhard) to design a formal and cryptographic proof of individual and universal verifiability of the protocol developed by the canton of Geneva, for a deployment in Switzerland.
- Docapost signed a 18-month contract in September 2017, with Pesto and Caramba, to enhance the voting solution of Docapost, in particular with respect to verifiability.

8.2. Bilateral Grants with Industry

A CIFRE contract with Numeryx has started with the Resist research group at Inria Nancy and Pesto, to develop algorithms for optimizing sets of filtering rules in Software Defined Networks.

PRIVATICS Project-Team (section vide)

PROSECCO Project-Team (section vide)

TAMIS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- CISCO (http://www.cisco.com) contract (2017–2022) to work on graph analysis of malware

8.2. Bilateral Grants with Industry

- CISCO (http://www.cisco.com) one grant (2016–2019) to work on semantical analysis of malware
- Thales (https://www.thalesgroup.com) one CIFRE (2016–2019) to work on verification of communication protocols, one grant (2018–2019) to work on learning algorithms
- Oberthur Technologies (http://www.oberthur.com/) one grant (2016–2020) to work on fuzzing and fault injection