RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2014

Section Popularization

Edition: 2015-03-26

Algorithmics, Computer Algebra and Cryptology

1. ARIC Project-Team . . . 5
2. CARAMEL Project-Team . . . 6
3. CASCADE Project-Team (section vide) . . . 7
4. CRYPT Team . . . 8
5. GALAAD2 Team (section vide) . . . 9
6. GEOMETRICA Project-Team . . . 10
7. GRACE Project-Team . . . 11
8. LFANT Project-Team . . . 12
9. POLSYS Project-Team . . . 13
10. SECRET Project-Team . . . 14
11. SPECFUN Project-Team . . . 15
12. VEGAS Project-Team . . . 16

Architecture, Languages and Compilation

13. ALF Project-Team (section vide) . . . 17
14. ATEAMS Project-Team . . . 18
15. CAIRN Project-Team (section vide) . . . 19
16. CAMUS Team . . . 20
17. COMPSYS Project-Team . . . 21
18. DREAMPAL Team . . . 22
19. GCG Team (section vide) . . . 23
20. PAREO Project-Team . . . 24
21. POSTALE Team . . . 25
22. TASC Project-Team . . . 26

Embedded and Real-time Systems

23. AOSTE Project-Team (section vide) . . . 27
24. CONVECS Project-Team . . . 28
25. HYCOMES Team (section vide) . . . 29
26. MUTANT Project-Team . . . 30
27. PARKAS Project-Team . . . 31
28. SPADES Team (section vide) . . . 32
29. TEA Project-Team (section vide) . . . 33

Proofs and Verification

30. ANTIQUE Team . . . 34
31. CELTIQUE Project-Team . . . 35
32. DEDUCTEAM Exploratory Action . . . 36
33. ESTASYS Exploratory Action (section vide) . . . 37
34. GALLIUM Project-Team . . . 38
35. MARELLE Project-Team . . . 39
36. MEXICO Project-Team . . . 40
37. PARSIFAL Project-Team (section vide) . . . 41

38. PI.R2 Project-Team 42
39. SUMO Project-Team (section vide) 43
40. TEMPO Team (section vide) 44
41. TOCCATA Project-Team 45
42. VERIDIS Project-Team 46

SECURITY AND CONFIDENTIALITY

43. CARTE Project-Team 47
44. CASSIS Project-Team 48
45. COMETE Project-Team 49
46. DICE Team 50
47. PRIVATICS Project-Team 51
48. PROSECCO Project-Team 52

ARIC Project-Team

9.4. Popularization

- Sylvie Boldo (Proval project) and Jean-Michel Muller wrote a popular science paper *Des ordinateurs capables de calculer plus juste* in the journal *La Recherche* [36].
- Nicolas Brisebarre co-organizes scientific conferences, called «Éclats de sciences», at Maison du Livre, de l'Image et du Son in Villeurbanne. Around three conferences take place per year.
- Nathalie Revol gave talks for pupils at collèges and lycées, as an incentive to choose scientific careers: lycée Camille Vernet (Valence, Drôme), lycée Jérémie de la Ville (Charlieu, Loire), lycée Gabriel Fauré (Annecy, Haute-Savoie), collège Jean Renoir (Neuville-sur-Saône, Rhône). During the "Week of mathematics", she gave a 2-hour talk at lycée de la Côtière (La Boisse, Ain). She gave the inaugural conference of the congress "Math en Jean's" in Lyon and the conference for the scientific camp "Math C2+" in Montbonnot. She was present for the "Mondial des Métiers" (Eurexpo Lyon, Chassieu, Rhône). For the Science Fair, she gave 2 talks at MMI, ENS de Lyon. In 2014, she met over 1000 pupils.

CARAMEL Project-Team

9.3. Popularization

- Jérémie Detrey gave a presentation on the Enigma machine and its cryptanalysis to high-school teachers as part as the “journée EPI-ISN”, where Paul Zimmermann gave a presentation of the Sage computer algebra system.
- Paul Zimmermann animated a “Maths-en-Jeans” group with students from the “collège” Pierre Brossolette in Réhon.
- Pierrick Gaudry gave a presentation at the “journée de l’Association francophone des spécialistes de l’investigation numérique”.
- Marion Videau
  - participated to events on information about university studies for pupils and students (Cap sur l’enseignement supérieur, Portes ouvertes de la faculté des sciences, Oriaction), and about university studies and research to the general public (Sciences en marche),
  - gave a presentation at the “journée de l’Association francophone des spécialistes de l’investigation numérique”.

CASCADE Project-Team (section vide)

CRYPT Team

6.3. Popularization

Phong Nguyen gave several invited talks:

- [17] at the First NTU-VIASM Workshop on Discrete Mathematics, in Vietnam.
- at the 2014 CTIC-IIIS Theory of Cryptography workshop, in China.
- at the Mathematical Workshop of the Chinese Association for Cryptologic Research, in China.

GALAAD2 Team (section vide)

GEOMETRICA Project-Team

9.3. Popularization

Thomas Bonis and Mathieu Carrière presented the *Photomaton 3d* at the *Fête de la Science* in October 2014. This animation consists in scanning a volunteering person in 3d using a Kinect and dedicated software, then illustrating the concepts of 3d shape comparison, retrieval and matching.

GRACE Project-Team

9.4. Popularization

- D. Augot made a presentation “Quand 1$\oplus$ 1 égal 0” at Lycée Albert Einstein, Sainte-Geneviève-des-Bois, May 19th.
- J. Pieltant was one of the presenters for Inria’s stand at « Bouge la Science » at Supélec.
- A. Couvreur gave a conference “Les mathématiques pour protéger l’information” for the pupils of Collège Moreau in Monthléry (91).

LFANT Project-Team

7.3. Popularization

K. Belabas gave a lecture to present Bhargava’s works (2014 Fields medal) to high school teachers during the “Journée de l’IREM d’Aquitaine” (11/2014, about 100 attendants).

A. Enge has presented “Les maths au service du secret (et de sa découverte!)” during the Math en Jeans congress held in Bordeaux in April 2014, for an audience of highschool pupils aged 12 to 17.

He has spoken on “Mathematik für (und gegen!) das Geheimnis” in an event in July at Gymnasium Leopoldinum, Detmold, Germany, to an audience comprised of pupils aged 12 to 18 and of mathematics teachers.

At the GNU Hacker’s Meeting 2014 in München, Germany, he has presented a tutorial on “GnuPG key signing”.

POLSYS Project-Team

8.4. Popularization

Guénaël Renault was invited speaker for the workshop *Fabriquer le Hazard du forum Science, Recherche et Société* (May 22, 2014) organized by the newspapers Le Monde et La Recherche.

SECRET Project-Team

9.3. Popularization

- Anne Canteaut has been invited to give the annual Computer Science Talk for the new students at Ecole Polytechnique, Palaiseau, June 2014 [79].

SPECFUN Project-Team

9.4. Popularization

- A. Mahboubi has written an article [16] for the popular science website “Images de Mathematiques”, in the context of a partnership of this website with the Bourbaki seminar.
- A. Mahboubi has given a talk at the popular science event “Nuit des Sciences, Ébullitions” http://www.nuit-sciences.ens.fr/ at École Normale Supérieure, on June 6th 2014.
- A. Mahboubi has been interviewed by Ph. Pajot in the magazine La Recherche, November 2014.
- A. Mahboubi has given a “Science Break” talk, at Supélec, on December 10th 2014, an event organized by La Diagonale Paris-Saclay, part of la Fondation de Coopération Scientifique Campus-Paris-Saclay.

VEGAS Project-Team

7.3. Popularization

Guillaume Moroz is a member of the organizing committee of the *Olympiades académiques de mathématiques*.

ALF Project-Team (section vide)

ATEAMS Project-Team

8.3. Popularization

Paul Klint:

- De Softwarerevolutie, Valedictory lecture.
- Nemo, Hoe ontstond de eerste computer?
- Nemo/Klokhuis, Hoe ontstond de eerste computer?
- BYOM: Bring Your Own Metrics (EQUA Symposium).
- The Revenge of the Coroutines (SEN Symposium).

Tijs van der Storm:

- Who’s afraid of Object Algebras?, Joy of Coding 2014.
- Hack your DSL with Rascal, CodeGeneration 2014.
- The Rascal Language Workbench, NSPyre, 2014.
- I am plain text, – resistance is futile, Sioux, 2014.
- Rascal: functional programming for source code analysis and transformation, guest lecture at Hogeschool van Arnhem en Nijmegen (HAN).

Jurgen Vinju:

- De allereerste computerprogrammeur Ada Lovelace (1815 - 1852), Kennis van NU (radio appearance).
- Complexe Software, Eindhovens Dagblad.
- De eerste programmeur, VPRO Gids.

Jan van Eijck is member of the Advisory Board (‘Raad van Advies’) of the Artificial Intelligence Curriculum, University of Groningen (since Summer 2013). Paul Klint acts as treasurer of the EAPLS and was directory of the Master Software Engineering at Universiteit van Amsterdam (UvA) until September 1, 2014. He is also board member of the Instituut voor Programmatuur en Algoritmiek (IPA). Tijs van der Storm is head of the internship committee at CWI, co-organizer of the CWI Scientific Meeting and secretary of the CWI works council.

CAIRN Project-Team (section vide)

CAMUS Team

9.3. Popularization

Cédric Bastoul participated to the event *Kids University* at the University of Strasbourg in November 2014

Cédric Bastoul prepared activities for *Fête de la Science* at University of Paris-Sud in October 2014

COMPSYS Project-Team

9.3. Popularization

- Alain Darte was invited to give a long keynote (1h30), as an introduction to polyhedral techniques ("Polyhedral optimizations? Not even scared!" [2]), to the spanish Conference Jornadas Sarteco, the equivalent of the french COMPAS conference, see http://www.jornadassarteco.org/transparencias-de-las-charlas-invitadas/.
- In Sep. 2014, together with ten other specialists in automatic parallelization, Paul Feautrier recorded a lecture on the "polyhedral model" for a video course on automatic parallelization to be published by the IEEE.
- Paul Feautrier's 1988 "Array Expansion" seminal paper has been selected for the 25th Anniversary Volume of the ACM International Conference on Supercomputing, with 34 other papers, among 1800 papers published from 1987 to 2011. A short "reminescence" paper [13] has been written for the occasion. http://dl.acm.org/citation.cfm?doid=2591635.2591641.
- Alain Darte participated to the "Refresh" Inria Rhône-Alpes initiative, for improving the scientific life of the Inria regional center, as well as to the working group on "team management".

DREAMPAL Team

8.3. Popularization

Philippe Marquet is vice-president of the *Société informatique de France*, the French learned society in computer science.

Philippe Marquet is involved in scientific popularization and co-animate the group of people interested in science popularization within the Inria Lille - Nord Europe Research Center. He is also of member of the group for networking about computer science popularization inside Inria.

He organizes and participates to the visit of classrooms on the Inria Plateau at EuraTechnologies, promoting interactions between the scientific community and secondary school students and their teachers. He organizes and/or animates events with children and/or adults in order to initiate them to code via Scratch or to computer science via unplugged activities (Poitiers, February 2014; Paris, October 2014; Inria Lille, December 2014).

Philippe Marquet is a member of the editorial board of 1024, the new bulletin of the *Société informatique de France* that aims at showing informatics, science and technology, in all its dimensions. 1024 targets a wide audience, from high school students to researcher, including anyone interested in computer science.

Hana Krichene participated in a contest "my thesis in 180 seconds", March 2014 - University Lille 1. The aim of the competition is to present the PhD student researches in simple terms in 3 minutes, with a clear, concise and convincing presentation to a diverse audience.

GCG Team (section vide)

PAREO Project-Team

8.3. Popularization

Jean-Christophe Bach participated to scientific mediation by proposing several activities to demonstrate the *algorithmic thinking* at the core of the Computer Science without requiring any computer or even electric devices. These activities are the first part of the CSIRL (Computer Science In Real Life) project which aims to popularize computer science and to initiate children, school students and non-scientists into this domain.

Pierre-Etienne Moreau gave two lectures about “Robotics and Programming” in the ISN course (Informatique et Science du Numérique), in order to help professors of “classes de terminale” to teach this discipline. He organized a three day course about “Algorithms, Programming and Databases” in order to help professors of “classes préparatoires aux grandes écoles” to teach this discipline.

Pierre-Etienne Moreau is member of the national committee for Inria “Médiation Scientifique”. He also participated to “Fête de la Science 2014” at Mines Nancy.

POSTALE Team

8.3. Popularization

Christine Eisenbeis est membre du conseil scientifique des programmes du centre d'Alembert, Centre Interdisciplinaire d'Étude de l'Évolution des Idées, des Sciences et des Techniques (CIEEIST), de l'université Paris-Sud. À ce titre, elle a fait partie du comité d'organisation du colloque "Recherche et démocratie", 21-22 mai 2014, Orsay, (http://www.centre-dalembert.u-psud.fr/archives-colloques/2014-recherche-scientifique-et-democratie/). Lors de l'animation "Livres au marché" de Malakoff, le 23 novembre 2014, elle a présenté, avec Jean-Pierre Archambault, le livre d'enseignement en terminale de l'ISN (Informatique et Sciences du Numérique) (principal auteur Gilles Dowek).

TASC Project-Team

9.3. Popularization

- A user guide is now available for CHOCO: 164 pages describing how to use CHOCO, together with a new website, see http://www.choco-solver.org. The next topics on the way will include:
  - Dealing with strong consistencies.
  - Designing an even more efficient free search strategy.
  - Providing a light explanation framework.
- Within the context of the global constraint catalog:
  - On-line interactive exercises completed (see http://imedia.emn.fr/global_constraints_course/).
  - Effort for providing more TikZ illustrations has been continued (about 1000 figures are currently available and 60 figures remain to be redesigned to TikZ) by Nicolas Beldiceanu.
  - Reorganization of the production of the pdf version (and enhancing look and navigation within the pdf) by Mats Carlsson.
  - Update of the web version (see http://sofdem.github.io/gccat/) by Sophie Demassey.
- A strong effort has also been made in 2014 to improve the dissemination of IBEX and the collaboration of programers. This includes:
  - Course on IBEX by Gilles Chabert at MACS 2015.
  - Creation of a new web site, see http://www.ibex-lib.org/.
  - Documentation writing (low-level interval arithmetic operations, contractors), see http://www.ibex-lib.org/doc/.
  - Migration of the code from SVN+sourceforge to github (github.com/ibex-team/ibex-lib).
  - Support via the new forum (http://ibex-lib.org/forum).
  - Bug/issue tracking system, private wiki for developers.
  - Introduction of Travis for continuous integration.
- Within the context of *Artificial Intelligence and real time strategy games*,
  - Interview by Inria Bretagne of F. Richoux on his work about Game AI, see emergences.inria.fr/emergences-2014/newsletter-n30/L30-STARCRAFT.
  - F. Richoux has been invited to write a short article about his work about Game AI in the “Bulletin de l’Association Française pour l’Intelligence Artificielle”. It should appear on January 2015.
- Presentation at the workshop les femmes dans le monde académique by Charlotte Truchet.
- A the 2014 edition of the Fête de la Science (Nantes University):
  - One talk on *Challenges around optimizations problems* was given by Xavier Lorca.
  - A session discussing and answering questions around the work of professor and researcher in computer science with young persons (18 years old) was spent by N. Beldiceanu.

AOSTE Project-Team (section vide)

CONVECS Project-Team

9.3. Popularization

H. Garavel participates to the committee in charge of organizing the Aerospace Valley series of industrial conferences on formal methods. The third conference [0], devoted to theorem proving, held on February 4 in Toulouse and retransmitted by video-conference in Grenoble, attracted over 100 participants from industry and academia.

The fourth conference [0], devoted to model checking, held on October 16 in Toulouse and retransmitted by video-conference in Grenoble and Saclay, attracted over 120 participants from industry and academia. H. Garavel gave a talk entitled "*Présentation de l'outil CADP*". A. Kriouile gave a talk entitled "*Application de CADP à la vérification de matériel*". R. Mateescu gave a talk entitled "*Introduction au model checking*".

[0] http://www.inria.fr/centre/grenoble/agenda/forum-methodes-formelles2
[0] http://projects.laas.fr/IFSE/FMF/J4/index.html

HYCOMES Team (section vide)

MUTANT Project-Team

8.3. Popularization

Arshia Cont was invited to a TEDx Talk in October 2014 on *Human-Computer Musicianship* that attracted more than 12 thousand podcasts according to organisers.

Arshia Cont was invited to participate 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.

Arshia Cont was invitee to the BFM Business Program on *Future of Sound*.

Arshia Cont was featured in the June Edition of *Usbek et Rica* magazine.

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

Article on Antescofo by Arshia Cont in the December 2014-January 2015 edition of the popular science magazine "Dossier de La Recherche".

José Echeveste, Arshia Cont and Jean-Louis Giavitto participated to the colloquium "La musique en temps réel" in the festival Musica, Strasbourg, september 2014.

Jean-Louis Giavitto participated to the colloquium "Le calcul et le temps, colloque de philosophie de l'informatique" Université Jean Moulin (Lyon 3), novembre 2014. He was invited on several seminars outside computer sciences: EPFL - ArchiZoom, "computational morphogenesis" in the context of the architecture exhibition "Animal ?" (april 2014); the e|m|a|fructidor art school in Chalons, "space and the formalization of musical processes" (april 2014); CNSMD Lyon and the Ecole Normale Lyon, "Du temps écrit au temps produit" with Julia Blondeau (april 2014); CISEC (club Inter-associations – AAAF, SEE, SIA – des Systèmes Embarqués Critiques), "Temps Réel en musique : Antescofo" (Toulouse June 2014).

Florent Jacquemard participated to the Inria seminar "1/2 hour of science" in July 2014, with a talk on Testing and Verification of interactive music systems.

PARKAS Project-Team

8.3. Popularization

T. Bourke hosted a tutorial by Makarius Wenzel at ENS Ulm on the Isabelle proof assistant.

SPADES Team (section vide)

TEA Project-Team (section vide)

ANTIQUE Team

9.3. Popularization

Mehdi Bouaziz gave a course on “Apprendre et enseignement — la programmation informatique des bibliothèques”, Maire de Paris, 12 hours, june-july 2014. Xavier Rival gave a talk on “Safety critical embedded softwares and their verification” at the Ceremony for the “Médailles of Engeniering Sciences” in April 2014. Xavier Rival participated to the organization of the “Nuit des Sciences” in June 2014.

CELTIQUE Project-Team

7.3. Popularization

- Talk “Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.”, Thomas Genet, for high school teachers, ENS Rennes, Oct. 2014.

DEDUCTEAM Exploratory Action

8.3. Popularization

Gilles Dowek is the president of the scientific board of the “Société Informatique de France” (SIF).

Gilles Dowek is a member of the scientific board of “La Main à la Pâte”.

Raphaël Cauderlier, Simon Cruanes, Pierre Halmagrand et Ronan Saillard ont participé à l’animation du stand Inria au Salon Culture et Jeux Mathématiques les 24 et 25 mai

Ali Asaf, Raphaël Cauderlier, Simon Cruanes et Pierre Halmagrand ont participé à l’animation du stand Inria lors de la Fête de la Science les 9 et 10 octobre 2014 à Paris

Gilles Dowek has given a talk at Mathenjeans.

Alejandro Díaz-Caro is member of the scientific board of “Ensemble”, a journal of the Maison Argentina at Cité Universitaire in Paris, ISSN 1852–5911.

ESTASYS Exploratory Action (section vide)

GALLIUM Project-Team

9.3. Popularization

Jacques-Henri Jourdan is involved in the organization of the Junior Seminar of Inria Paris-Rocquencourt.

Jacques-Henri Jourdan manned a stand at “Salon Culture & Jeux Mathématiques”, in Paris.

Since 2012, the Gallium team publishes a research blog at http://gallium.inria.fr/blog/, edited by Gabriel Scherer. This blog continued its activity in 2014, with 23 posts from 5 different authors.

MARELLE Project-Team

9.4. Popularization

Laurent Théry presented his researcher work to three different classrooms during the event "semaine des maths", in March.

MEXICO Project-Team

9.3. Popularization

- Stefan Haar gave a talk entitled "Revèle tes défauts" on fault diagnosis in the popularization series "Unithé ou café" of Inria Saclay-Idf, on February 7, 2014.

PARSIFAL Project-Team (section vide)

PI.R2 Project-Team

7.3. Popularization

Pierre-Louis Curien wrote the editorial of a special “hors série” issue of the information letter of The Fondation Sciences Mathématiques, entitled “Des preuves et des programmes”, may 2014. He wrote an introductory article “Formalisation mathématique, certification logicielle, même combat!” in the journal Gazette des Mathématiciens 142, 83-86 (octobre 2014).

Lourdes González-Huesca and Étienne Miquey took part in the animation of the “Fête de la Science” event at the University Paris 7.

Étienne Miquey took part in the animation of several activities about mathematics in elementary and high schools of Paris.

Yann Régis-Gianas co-organised the “Journée Francilienne de Programmation”, a programming contest between undergraduate students of three universities of Paris (UPD, UPMC, UPS).

Yann Régis-Gianas organised the “Fête de la Science” event for the computer science department of the University Paris 7.

Yann Régis-Gianas and Pierre Letouzey took part in the “Salon Culture et Jeux mathématiques” at Saint Sulpice, Paris.

Yann Régis-Gianas gave several conferences about “What is programming?” in elementary and high schools of Paris.

SUMO Project-Team (section vide)

TEMPO Team (section vide)

9.3. Popularization

- S. Boldo presented the *Concours Castor informatique* to computer sciences teachers (ISN) in Nancy on April 17th, 2014. A video of the talk is available at http://videos.univ-lorraine.fr/index.php?act=view&id=1369.
- S. Boldo gave a 2-hour course entitled *Les nombres et l'ordinateur* at the École Normale Supérieure de Cachan, France, on September 9th.
- S. Boldo gave a 2-hour course *Pourquoi mon ordinateur calcule faux?* to a general audience at the Université Inter-Âge in Versailles, France, on March 4th.
- S. Boldo gave a talk for computer sciences teachers (ISN) in Créteil on March 24th
- S. Boldo gave a talk for teenagers at the lycée Maximilien Perretin Alfortville on May 22nd.
- S. Boldo wrote an article with Jean-Michel Muller (ARIC) in the popularization journal La Recherche [42].
- S. Boldo wrote in 2013 an article for the French blog celebrating 2013 as the "Mathematics of Planet Earth" year: http://mpt2013.fr/meme-les-ordinateurs-font-des-erreurs/. This article was selected to be published in a book published in 2014 [41].
- S. Boldo is member of the editorial committee of the popular science Interstices web site, since April 2008. http://interstices.info/.
- S. Boldo is member of the editorial board of Binaire http://binaire.blog.lemonde.fr, the blog of the French Computer Science Society.
- S. Boldo, G. Melquiond, A. Paskevich, and C. Paulin animated two stands at the *Fête de la science*.
- A. Charguéraud and S. Boldo contributed to the preparation of the exercises of the *Concours Castor informatique*http://castor-informatique.fr/. A. Charguéraud is also one of the three organizers of this contest. The purpose of the Concours Castor in to introduce pupils (from *6ème* to *terminale*) to computer sciences. More than 228,000 teenagers played with the interactive exercises in November 2014.
- S. Conchon and J.-C. Filliâtre published a book *"Apprendre à programmer avec OCaml"* for undergraduate students learning computer programming [39] (Eyrolles, September 2014).

VERIDIS Project-Team

9.3. Popularization

Marie Duflot-Kremer took part in various popularization activities, with a public ranging from primary school kids (with unplugged activities concerning sorting, programming, error detection) to non-scientific staff of the Inria center. She is also a member of the steering committee preparing an itinerant exposition intended for explaining computer science to high-school students and took part in an event of the European Code Week in Paris.

Pascal Fontaine and Stephan Merz illustrated some subjects and techniques that underly formal verification of protocols and algorithms at events like “Fête de la Science”. Using wooden puzzles and Sudoku sheets, they explained how real-life problems can be represented in logical form and then solved using automated tools based on formal logic.

Christoph Weidenbach lectured within the series “Perspektiven der Informatik” at Saarland University and within the public lecture series of the federal state of Saarland.

CARTE Project-Team

8.3. Popularization

Isabelle Gnaedig is member of the scientific vulgarization committee of Inria Nancy - Grand Est. This committee is a choice and guidance instance helping the direction of the center and the person in charge of popularization events to elaborate a strategy, to realize events and to help researchers to get involved in various actions aiming at popularizing our research themes, and more generally computer science and mathematics.

CASSIS Project-Team

9.3. Popularization

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

COMETE Project-Team

8.3. Popularization

Catuscia Palamidessi has organized the round table “Security & Privacy : challenges of the future digital society” at the Forum STIC, University of Paris-Saclay, December 2014.

Konstantinos Chatzikokolakis has been one of the speakers at the above round table.

Konstantinos Chatzikokolakis has given the popularization talk “Protection de la vie privée et anonymat” at the Journée ISN, Académie de Créteil, March 2014.

DICE Team

8.3. Popularization

- Stéphane Frénot and Stéphane Grumbach have been invited speakers to the BlendWebMix conference in Lyon end of October. This event of two days unites actors from different fields in the web domain, i.e. programmers, entrepreneurs, designers and scientists. Two contributions have been programmed for DICE to speak about digital and geographical territories, and about big data and intermediation platforms.
- The annual German-speaking conference DNP14 in Vienna (Austria) is a two-day event to discuss topics related to data, networks and politics and has taken place this year in September. Robert Riemann was giving a talk to introduce the concept of the C3PO project and illustrate its possibilities of application.
- Metroscope aims at being a leading Internet Observatory. It holds an annual workshop. Aurélien Faravelon presented DICE's works on intermediation at the 2014 edition.
- Séminaire Pint Of Science, Lyon, Google, Twitter, BitTorrent et BitCoin : les données, objets de toutes les convoitises http://www.pintofscience.fr/#!lyon/ci18, 21 Mai 2014
- Rencontres CNRS Journées citoyen CNRS, poitiers, invitation to a seminar at school about Big Data, 17-19 Oct 2014, http://www.cnrs.fr/sciencesetcitoyens/
- Panel Big Data, Open Data : enjeux démocratiques, colloque Le monde après Snowden, Assemblée nationale, Paris, 13-14 mars 2014
- La France dans le paysage mondial de l'intermédiation, Audition publique au Sénat, Mission commune d'information "Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet", Paris, 11 Febr 2014
- Les enjeux du numérique présentés aux députés, avec la délégation Inria, et le groupe d'études Internet et société numérique de l'Assemblée nationale, Paris, 21 janvier 2014

PRIVATICS Project-Team

8.3. Popularization

Interview of Mathieu Cunche on Radio Canada in the chronicle of Janic Tremblay, 3rd February 2014.

Interview of Mathieu Cunche on Radio France Inter in “Journal de 18h”, February 28th 2014.

Seminar of Mathieu Cunche “ Je sais tout sur vous grâce au Wi-Fi! ” Séminaire sur la Confiance Numérique at Clermont Ferrand, March 6th, 2014.

Interview of Mathieu Cunche on Radio France Info in “Tout comprendre” chronicle, March 18th, 2014.

Interview of Mathieu Cunche in Ouest-France news-paper, May 10th, 2014.

Participation of Mathieu Cunche to the TV show "Le Monde en Face" on France 5, June 17th, 2014.

Participation of Mathieu Cunche to the round table “ Numériquement vôtre ” at Futur en Seine, June 14h, 2014.

Seminar of Mathieu Cunche “ Internet: Vie privée, Surveillance et Censure ” at St-Génis Les Ollières, December 20th, 2014.

Seminar of Cédric Lauradoux “ Identifiants et guesswork ” Séminaire sur la Confiance Numérique at Clermont Ferrand, January 9th, 2014.

Seminar of Cédric Lauradoux “ Identifiants et guesswork ” Séminaire sur la Confiance Numérique at Clermont Ferrand, January 9th, 2014.

Seminar of Cédric Lauradoux “ Déni de Service Algorithmique ”, Journées Sécurité des Systèmes d’informations at Rouen, November 13th, 2014.

Seminar of Cédric Lauradoux “ L’Internet des Objets et l’Internet des identifiants ”, Colloque Sćurité de l’Internet des Objets (chaire de cyberdéfense et cybersécurité Saint-Cyr – Sogeti – Thalès) at Rouen, September 19th, 2014

Interview of Vincent Roca and Mathieu Cunche, “ Comment brouiller sa trace dans les réseaux ? ” Sciences et Avenir, issue 809, July 2014.

Interview of Vincent Roca, “ Spécial Grenoble : portrait de trois chercheurs ”, Le Point édition régionale, issue 2195, October 9th, 2014.

Editorial of Claude Castelluccia and Vincent Roca, “ Mobilitics Saison 2: les smartphones et leurs apps sous le microscope de la CNIL et d’Inria ”, La lettre Innovation et Prospective de la CNIL, issue 8, December 2014.

Seminar of Vincent Roca, “ Vie privée et Smartphone : le projet Mobilitics Inria/CNIL ”, DAFP-RAF Inria meeting, Paris, October 16th, 2014.

Seminar of Vincent Roca, “ Vie privée et Smartphone : le projet Mobilitics Inria/CNIL ”, organized by the Guilde des Utilisateurs d’Informatique Libre du Dauphiné (GUILDE), Grenoble, November 4th, 2014.

Short TV subject with Vincent Roca, “ Applications mobiles : de vrais espions ? ”, ARTE X:enius magazine, September 1st, 2014. http://www.arte.tv/guide/fr/051090-010/x-enius?vid=051090-010_PLUS7-F

Press conference, organized by CNIL in association with Inria, “ Vie privée et smartphones : les nouveaux résultats du projet Mobilitics Inria-CNIL ”, December 15th, 2014.

Seminar of Daniel Le Métayer, at the Cybersecurity Forum (ETH Zurich), 2014.

Participation of Daniel Le Métayer to a panel on privacy by design at the Annual Privacy Forum (APF 2014, Athens).

Participation of Daniel Le Métayer to Panel on at Computers Privacy and Data Protection (CPDP 2014 – Brussels).

Nomination of Daniel Le Métayer at the Commission of the French Parliament “Commission de réflexion et de propositions ad hoc sur le droit et les libertés à l’âge du numérique. ”

Organization of a seminar on privacy for the COERLE (Inria) by Claude Castelluccia and Daniel Le Métayer, November 2014.

PROSECCO Project-Team

8.3. Popularization

8.3.1. Seminars

- Graham Steel: invited talks at FCS-FCC 2014 (Vienna)
- Graham Steel: invited keynote at Grande Region security day (Saarbrucken).
- Bruno Blanchet: invited talk at the Dagstuhl seminar “The synergy between programming languages and cryptography”.
- Karthikeyan Bhargavan: invited talk at the IETF TLS Working Group to discuss the Triple Handshake Attack (London)
- Karthikeyan Bhargavan: invited talk at the Dagstuhl seminar “The synergy between programming languages and cryptography”.
- Karthikeyan Bhargavan: invited talk at Les Journées Scientifiques Inria in Lille
- Karthikeyan Bhargavan: invited panelist at Security Standardization Research workshop in Surrey UK
- Karthikeyan Bhargavan: invited keynote at Santa’s Crypto Workshop 2014 (Prague)
- Antoine Delignat-Lavaud: briefing at BlackHat USA on “The BEAST Wins Again: Why TLS Keeps Failing to Protect HTTP”
- Catalin Hritcu: invited keynote at Grande Region security day (Saarbrucken).
- Catalin Hritcu: seminar at Groupe de travail LTP du GDR GPL
- Catalin Hritcy: seminar at Groupe de travail Théorie des types et réalisabilité

8.3.2. Vulnerabily Reports

- Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Alfredo Pironti reported the so-called Triple Handshake attacks on TLS implementations leading to security updates to all major web browsers: Google Chrome (CVE-2013-6628), Mozilla Firefox (CVE-2014-1491), Internet Explorer (CVE-2014-1771), Apple Safari (CVE-2014-1295), as well as to non-browser TLS libraries such as Oracle JSSE (CVE-2014-6457) and RSA BSAFE (CVE-2014-4630). For more details, see http://secure-resumption.com
- Antoine Delignat-Lavaud reported virtual host confusion attacks on a number of web servers, leading to security updates to the Akamai content delivery network, Dropbox, Bugzilla, as well as the NGINX web server. His results were presented at BlackHat USA and are summarized at http://bh.ht.vc
- Karthikeyan Bhargavan reported state machine attacks on major TLS libraries, such as OpenSSL (CVE-2014-3572), NSS, JSSE, CyaSSL, and SecureTransport, leading to security updates in all these libraries.