imdea software institute

science and technology for developing better software

institute
imdea
software

annual report 2014

imdea software institute

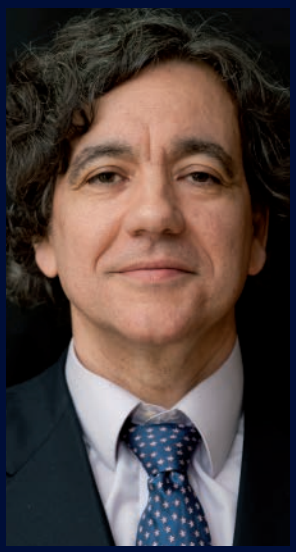
science and technology for developing better software

institute
imdea
software

annual report 2014

foreword

foreword



Manuel Hermenegildo
Director, IMDEA Software Institute
March 15, 2015

annual report
2014

The IMDEA Software Institute was created by the Madrid Regional Government under the strong belief that quality research in technology-related areas is the most successful and cost-effective way of generating knowledge, sustainable growth, and employment. This is more relevant currently than ever, and software-related technology indeed has an immense potential for raising industrial competitiveness, opening whole new business areas, creating high added-value jobs, and improving quality of life. Today, the Institute is a vibrant, exciting reality, reaching significant milestones within its objectives of excellence in research and technology transfer.

Without any doubt, the main strength of the Institute is its people: its researchers and support staff. The Institute has been very successful in attracting to Madrid top talent worldwide, including now 20 faculty (one half-time), 9 postdocs, 24 research assistants, 6 project staff, a number of interns, and 10 staff members, from 16 different nationalities. Our researchers have joined the Institute after working at or obtaining their Ph.D. degrees from 32 different prestigious centers in 8 different countries, including Stanford U., Carnegie Mellon U., or Microsoft Research in the US, INRIA in France, U. of Cambridge in the UK, the Max Planck Software Institute in Germany, or ETH in Switzerland, to name just a few. In addition, more than 130 international researchers have visited and given talks at the Institute to date.

During 2014 Institute researchers have published 74 refereed publications (in some of the top venues in the field, such as POPL, CRYPTO, IEEE S&P, CAV, TPLP, ICLP, ICALP, etc.), given 17 invited talks and 30 invited seminars and lectures, and participated in 51 program committees and 15 boards of journals and conferences, in addition to being conference or program chairs of 6 conferences. The Institute has received 8 best paper awards or mentions in the last 4 years.

The Institute has also participated during 2014 in 29 funded research projects and contracts and received 15 fellowships. 15 of the projects are from international agencies (14 funded by the EU, 1 by the US ONR and Stanford U.), 8 are direct industrial funding, and 79% of them (23) involve collaboration with a large number of companies which include Atos, Siemens, Deimos, AbsInt, Microsoft, Fredhopper, Telefonica, Boeing, Thales, Reply, Maxeler, XMOS, and Logicblox (and many others in other recent projects, such as France Telecom, SAP, Trusted Logic, Airbus, Alcatel, Daimler, or EADS). The Institute is also working on the commercialization of the ActionGUI technology (developed by its Modeling Lab) in collaboration with ETH Zurich.

In 2014 the Institute has also strengthened its strategic partnership with Telefonica, Indra, Atos, UPM, and BSC, including a significant increase of the activities of the European Institute of Technology (EIT) ICT Labs Spanish Associate Partner Group, with an important expansion of the Madrid Co-Location Center, hosted and run by the Institute, and many other joint activities in innovation and entrepreneurship. The Institute has also continued its strong collaborations with Microsoft within the Microsoft Research–IMDEA Software Joint Research Center. In the context of these activities, during 2014 the Institute has hosted a good number of research and entrepreneurship events, including for example the Microsoft-IMDEA Software Collaboration Workshop or the CDTI - IMDEA Software H2020 Info-Day on Entrepreneurship.

Many thanks once more to all who have contributed to all these achievements, and very specially to the Madrid Regional Government for their continuing vision and support.

table of contents

table of contents

annual report

2014

1. General Presentation [6]
2. Industrial and Institutional Partnerships [14]
3. Research [24]
4. People [37]
5. Research Projects and Contracts [60]
6. Dissemination of Results [75]
7. Scientific Highlights [93]

general presentation

1.1. Profile [7]

1.2. Motivation and Goals [7]

1.3. Legal Status, Governance, and Management [8]

1.4. Appointments to the Board of Trustees [10]

1.5. Members of the Governing Bodies [10]

1.6. Headquarters Building [12]

1.1. Profile

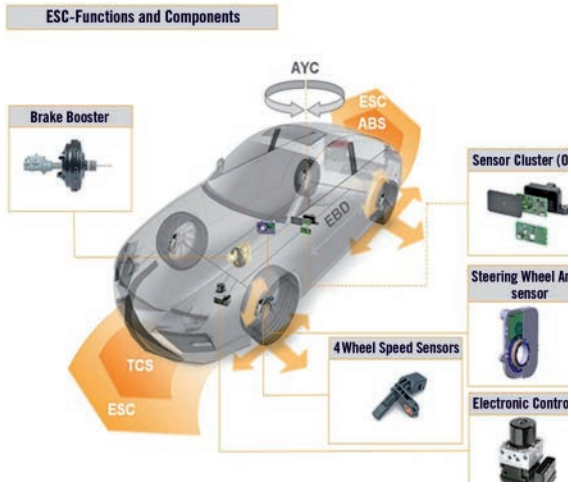
The IMDEA Software Institute (Madrid Institute for Advanced Studies in Software Development Technologies) is a non-profit, independent research institute promoted by the Madrid Regional Government (CM) to perform research of excellence in the methods, languages, and tools that will allow the cost-effective development of software products with sophisticated functionality and high quality, i.e., which are safe, reliable, and efficient.

The IMDEA Software Institute is part of the Madrid Institute for Advanced Studies (IMDEA) network, an institutional framework created to foster social and economic growth in the region of Madrid by promoting research of excellence and technology transfer in a number of strategic areas (water, food, energy, materials, nanoscience, networks, and software) with high potential impact.

1.2. Motivation and Goals

It is difficult to overstate the importance of software in both our daily lives and in the industrial processes which, running behind the scenes, sustain the modern world. Indeed, software is the enabling technology behind many devices and services that are now essential components of our society, ranging from large critical infrastructures on which our lives depend (cars, planes, air-traffic control, medical devices, banking, the stock market, etc.) to more mundane devices which are now an essential part of our lives (like cell phones, tablets, computers, digital televisions, and the Internet itself). Software has not only facilitated improved solutions to existing problems, but has also started modern revolutions like social networks that change the way we communicate and interact with our environment and other humans. This pervasiveness explains the global figures around software and the IT services sector: according to the Gartner Worldwide IT Spending Forecast published at the end of 2014, global IT spending in 2015 is expected to grow by 2.4% and exceed 3.8 trillion USD, with the annual growth rate close to 3% for the 2016-18 period. According to European Commission data for 2014, the EU digital economy is growing at 12% each year, and has already surpassed in size the national economy of a mid-sized member country like Belgium. The same source argues that approximately half of EU productivity growth comes from investment in ICT, and that the Internet economy creates five new jobs for every two '*offline*' jobs lost. This vividly illustrates the huge potential of ICT to drive economic growth and create jobs.

Given the economic relevance of software and its pervasiveness, errors and failures in software can have high social and economic cost: the results of malfunctioning software can range from being annoying (e.g., having to reboot), through posing serious social and legal problems (e.g., privacy and security leaks), to having high economic cost (e.g., software failures in financial markets and software-related product recalls) or even being a threat to human



Modern cars and trucks contain as many 100 million lines of computer code. This software runs on more than 30 on-board computers and controls vital functions, including the brakes, engine, cruise control, and stability systems. It is under increasing scrutiny in the wake of recent problems with major manufacturers and it is currently impossible to fully test.

lives (e.g., a malfunctioning airplane or medical device). Unfortunately, developing software of an appropriate level of reliability, security, and performance, at a reasonable cost is still a challenge today. A recent study from Cambridge University found that the global cost of debugging software has risen to $312 billion annually, while other studies estimated the cost to just the US U.S. economy at $60 billion annually, or about 0.6 percent of GDP. The reason for this high cost is that, while some degree of software correctness can be achieved by careful human or machine-assisted inspection, this is still a labor-intensive task requiring highly qualified personnel, with the ensuing high monetary price. Even worse, the risk of errors produced by human mistakes will still be lurking in the dark. Reducing software errors in a cost-effective manner is therefore a task that can greatly benefit from the development of automatic tools. However, such tools are extremely hard to produce, because their design and construction poses scientific and technological challenges. At the same time, the ubiquity of software makes taking on these challenges a potentially highly profitable endeavor, since solutions to these problems can have a significant and pervasive impact on productivity and on the general competitiveness of the economy.

The main mission of the IMDEA Software Institute is to tackle these challenges by performing research of excellence in methods, languages, and tools that will allow developing software products with sophisticated functionality and high quality, i.e., software products that are at the same time secure, reliable, and efficient, while ensuring that the process of developing such software is also highly cost-effective. A distinctive feature of the Institute is the concentration on approaches that are rigorous and at the same time allow building practical tools. The research focus includes all phases of the development cycle (analysis, design, implementation, validation, verification, maintenance).

In order to achieve its mission, the IMDEA Software Institute gathers a critical mass of worldwide, top-class researchers, and at the same time develops synergies between them and the

already significant research base and industrial capabilities existing in the region. Indeed, most of the IT-related companies in Spain (and, specially, their research divisions) are located in the Madrid region, which facilitates collaboration and technology transfer. Thus, the IMDEA Software Institute materializes the opportunity of grouping a critical mass of researchers and industrial experts, allowing for significant improvement in the impact of research.

1.3. Legal Status, Governance, and Management

The IMDEA Software Institute is a non-profit, independent organization, constituted as a Foundation. Its structure brings together the advantages and guarantees offered by a foundation with the flexible and dynamic management typical of a private body. This combination is deemed necessary to attain the goals of excellence in research, cooperation with industry, and attraction of talented researchers from all over the world, while managing a combination of public and private funds. The Institute was created officially on November 23, 2006 at the initiative of the Madrid Regional Government, following a design that was the result of a collaborative effort between industry and academia, and started its activities during 2007.

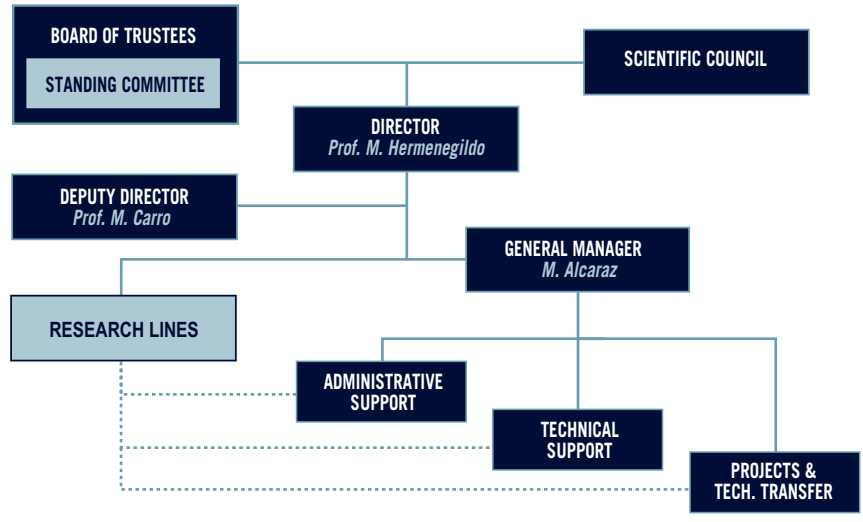


Figure 1.1. Governance and management structure of the IMDEA Software Institute.

The main governing body of the Institute is the **Board of Trustees**. The Board includes representatives of the Madrid Regional Government, universities and research centers of Madrid, scientists with high international reputation in software development science and technology, and representatives of companies, together with independent experts.

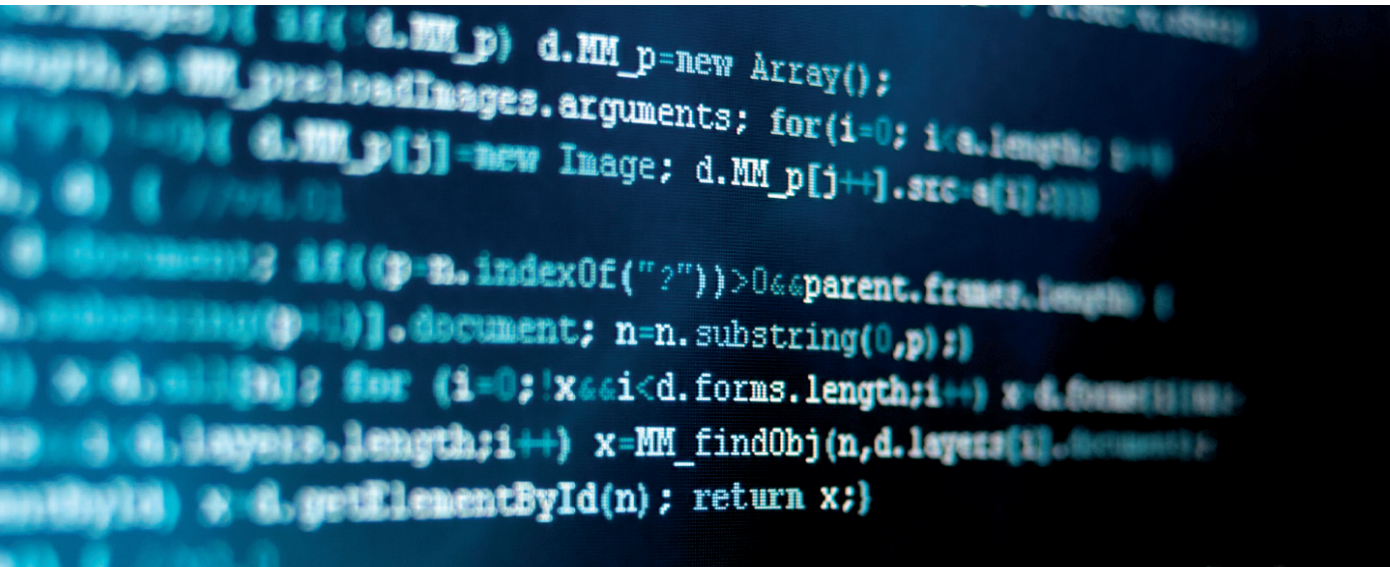
The Board is in charge of guaranteeing the fulfillment of the foundational purpose and the correct administration of the funds and rights that make up the assets of the

Institute, maintaining their appropriate returns and utility. The Board normally meets twice a year. In the interim, Board-level decisions are delegated to the **Standing Committee** of the Board. The Board appoints the **Director**, who is the CEO of the Institute, among scientists with a well-established international reputation in software development science and technology. The Director fosters and supervises the activities of the Institute, and establishes the distribution and application of the available funds among the goals of the Institute, within the patterns and limits decided by the Board of Trustees. The Director is assisted by the **Deputy Director** and the **General Manager**, who take care of the legal, administrative, and financial activities of the Institute, and supervise the **Project Management and Technology Transfer** unit and the **Technical Support and Research Infrastructure** unit, which work closely with and support the **Research Lines** of the Institute. The current structure is depicted in Figure 1.1.

The Board of Trustees and the Director are assisted in their functions by the **Scientific Council**, composed of high-level external scientists of international reputation with expertise in different areas of research covered by the Institute. The tasks of this scientific council include: to provide advice on and approve the selection of researchers; to provide advice and supervision in the preparation of yearly and longer-term strategic plans; to evaluate the performance with respect to those plans; and to give general advice on matters of relevance to the Institute.

1.4. Appointments to the Board of Trustees

During 2014, Rocio Albert Lopez-Ibor, former Director General for Universities and Research of the Madrid Region, was appointed Vice-Counselor for Innovation, Industry, Commerce, and Consumption of the Madrid Region, and was replaced in the board by Lorena Heras Sedano, the new Director General for Universities and Research. Also in 2014, Víctor Robles Forcada took over from Javier Segovia Pérez as the representative of the Technical University of Madrid (UPM).



1.5. Members of the Governing Bodies

Board of Trustees

CHAIRMAN OF THE FOUNDATION

Prof. David S. Warren
State University of New York at Stony Brook, USA.

VICE-CHAIRMAN OF THE FOUNDATION

Excma. Sra. Dña. Alicia Delibes Liniers
Vice-counselor for Education, Madrid Regional Government, Spain.

MADRID REGIONAL GOVERNMENT

Excma. Sra. Dña. Alicia Delibes Liniers
Vice-counselor for Education, Madrid Regional Government, Spain.

Ilmo. Sr. D. José María Rotellar García
Vice-counselor of the Treasury, Madrid Regional Government, Spain.

Ilma. Sra. Dña. Lorena Heras Sedano
Director General for Universities and Research, Madrid Regional Government, Spain.

Prof. Juan Ángel Botas Echevarría
Deputy Director for Research, Department of Education, Madrid Regional Government, Spain. Chairman of the Standing Committee.

UNIVERSITIES AND PUBLIC RESEARCH BODIES

Prof. Narciso Martí Oliet
Universidad Complutense de Madrid, Spain.

Prof. Víctor Robles Forcada
Universidad Politécnica de Madrid, Spain.

Prof. Diego Córdoba Gazolaz
Consejo Superior de Investigaciones Científicas (CSIC), Spain.

Prof. Jesús M. González Barahona
Universidad Rey Juan Carlos, Madrid, Spain.

SCIENTIFIC TRUSTEES

Prof. David S. Warren
State University of New York at Stony Brook, USA. Chairman of the Board of Trustees.

Prof. Patrick Cousot
Courant Institute, New York University, USA.

Prof. Luis Moniz Pereira
Universidade Nova de Lisboa, Portugal.

Prof. José Meseguer
University of Illinois at Urbana Champaign, USA.

Prof. Roberto Di Cosmo
Université Paris 7, France.

EXPERT TRUSTEES

Mr. José de la Sota Rius
Managing Director, Fundación para el Conocimiento (MadrI+D), Madrid, Spain.

Mr. Eduardo Sicilia Cavanillas
Escuela de Organización Industrial, Madrid, Spain.

INDUSTRIAL TRUSTEES

BBVA
Ms. María del Carmen López Herranz, Global Head of Branch Technology at BBVA.

Board meetings have been attended, as invitees, by representatives of the following companies:

Telefónica I+D
Mr. Francisco Jariego, Director for Industrial Internet of Things, Telefónica Digital.

Deimos Space
Mr. Miguel Belló Mora, General Director, and Mr. Carlos Fernández de la Peña.

Atos
Mr. José María Cavanillas, Director for Research & Innovation, and Ms. Clara Pezuela.

SECRETARY

Mr. Alejandro Blázquez Lidoy

Scientific Council

Prof. David S. Warren
State University of New York at Stony Brook, USA.
Chairman of the Board.

Prof. María Alpuente
Universidad Politécnica de Valencia, Spain.

Prof. Roberto Di Cosmo
Universitè Paris 7, France.

Prof. Patrick Cousot
Courant Institute, New York University, USA

Prof. Veronica Dahl
Simon Fraser University, Vancouver, Canada.

Prof. Herbert Kuchen
Universität Münster, Germany.

Prof. José Meseguer
University of Illinois at Urbana Champaign, USA.

Prof. Luis Moniz Pereira
Universidade Nova de Lisboa, Portugal.

Prof. Martin Wirsing
Ludwig-Maximilians-Universität, München, Germany.

1.6. Headquarters Building

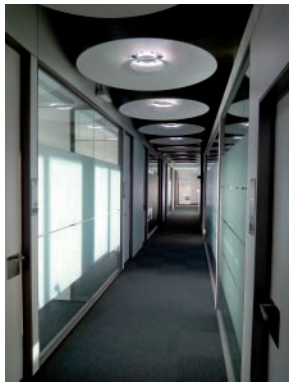
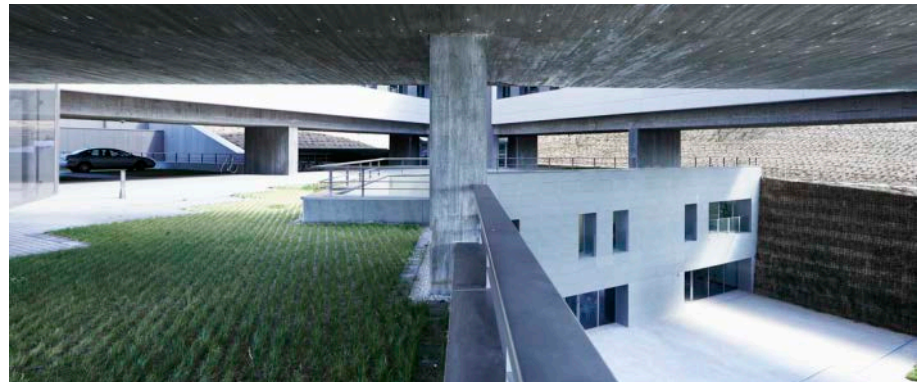
Since 2013, the IMDEA Software Institute is located in its new headquarters building in the Montegancedo Science and Technology Park, which was officially inaugurated in July 2013. The new building offers an ideal environment for fulfilling its mission of research and technology transfer. It includes offices, numerous spaces for interaction and collaboration, areas for project meetings and for scientific and industrial conferences and workshops, and powerful communications and computing infrastructures. It also provides ample space for strategic activities such as the Madrid Co-location Center of the European Institute of Technology ICT Labs, the IMDEA Software-Microsoft Joint Research Center, the IMDEA Software-Telefonica Joint Research Unit, and other joint research units with industry. It is highly energy-efficient, through energy-conscious design, co-generation, and full automation.

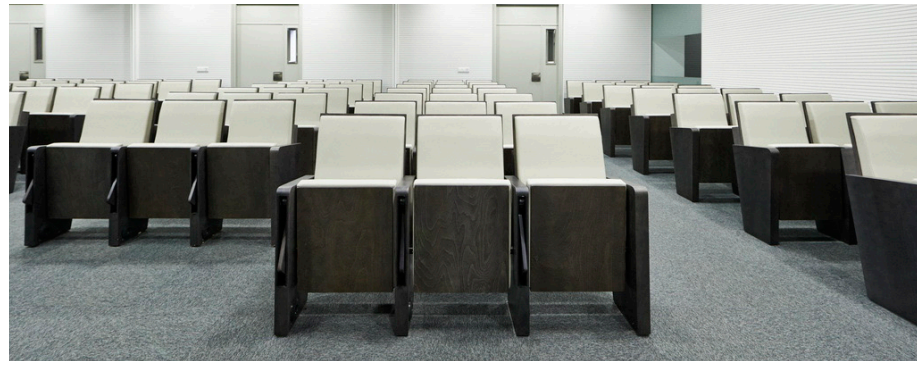
The location of the new IMDEA Software building also provides excellent access to the UPM Computer Science Department as well as to the other research centers within the Montegancedo Park. These centers include the Madrid Center for Supercomputing and Visualization (CESVIMA), the UPM Montegancedo Campus company "incubator" and technology transfer center (CAIT), the Institute for Home Automation (CEDINT), the Institute for Biotechnology and Plant Genomics (CBGP), the Center for Biomedical Technology (CTB), the Microgravity Institute, and the Spanish User

Support and Operations Centre for ISS payloads (USOC). In particular, the CESVIMA houses the second largest supercomputer in Spain and one of the largest in Europe, as well as a state-of-the-art visualization cave, and is equipped for massive information storage and processing, high performance computing, and advanced interactive visualization.

The campus recently obtained the prestigious "International Campus of Excellence" label, and is the only campus in Spain to receive a "Campus of Excellence in Research and Technology Transfer" award in the Information and Communications Technologies area from the Spanish government.





industrial and institutional partnerships

2.1. Industrial Partnerships [15]

2.2. Cooperation with Research Institutions [18]

2.3. EIT ICT Labs [19]

2.4. Microsoft Research - IMDEA Software Joint Research Center [21]

2.5. Telefónica - IMDEA Software Joint Research Unit [22]

2.6. REDIMadrid [22]

annual report 2014

2.1. Industrial Partnerships

The key to innovation is in incorporating new scientific results and technologies into processes and products in a way that increases the competitiveness of industry, contributes to sustainable growth, and creates jobs. As a generator of new knowledge and technology in the area of ICT –which has a high economic impact– IMDEA Software is committed to fostering innovation and technology transfer in partnership with industry.

Key instruments of industrial partnership are focused collaborations with companies in the form of both collaborative projects funded through competitive public calls and direct industrial contracts. These instruments represent an excellent vehicle for performing joint research and pushing its results towards the market. Figure 2.1 lists some of the companies with which the IMDEA Software Institute has collaborated to date in such projects and contracts. The currently active projects and contracts are described further in Chapter 5.

The Institute has also established *strategic partnerships* with the main stakeholders in the sector which facilitate longer-term collaboration across projects. In particular, the Institute has established close ties with Telefonica, Indra, Atos, and BBVA which have led to a number of strategic cooperation initiatives. An important instance is the joint establishment of the European Institute of Technology (EIT) ICT Labs Spanish Associate Partner Group (with participation also of UPM and BSC), coordinated by the Institute, which includes the hosting and operation of the the EIT ICT Labs Madrid Co-Location Center and many other joint activities in innovation and entrepreneurship. In addition, the Institute has established the with Telefónica *Telefónica-IMDEA Software Joint Research Unit* and with Microsoft the *Microsoft Research–IMDEA Software Joint Research Center*, and is planning the establishment of more such units with other industrial partners. These activities are described in more detail later.

ICT SECURITY & TRUST

Madrid Network

eit EIT ICT Labs

es.INTERNET

Participation in Spanish and EU *Technology Platforms* is another strategically important line of cooperation with industry. Such platforms include the Technology Clusters of the Madrid Region, and the Internet of the Future *Es.Internet* Spanish platform. All these activities contribute towards aligning research agendas and promote joint participation in projects.

Another important form of technology transfer is the *commercialization of technology* developed at the Institute. Given the controversy around software patents (and the difficulties for filing software patents in Europe) the Institute is combining the protection of its intellectual property with other innovative exploitation models, such as those based on open-source or free software licenses, together with the licensing of such technology, and the *creation of technology-based start-ups*. For example, five *software registrations* have been completed to date, including ActionGUI (jointly developed by IMDEA Software and ETH Zurich, for which joint work on its commercialization is under way); GGA; and EasyCrypt, ZooCrypt, and Masking (the latter three developed jointly by IMDEA Software and INRIA).

Project/Contract	Funding Entity	Industrial Partners
MOBIUS	FP6: IP	France Telecom, SAP AG, Trusted Labs
HATS	PF7: IP	Fredhopper
NESSoS	PF7: NoE	Siemens, ATOS
ES_PASS(Through an associated group at UPM.)	ITEA2, MITyC	Airbus France, Thales Avionics, CS Systèmes d'Information, Daimler AG, PSA Peugeot Citroen, Continental, Siemens VDO Automotive, EADS Astrium, GTD, Thales Transportation, and IFB Berlin
EzWeb	MITyC	Telefónica I+D, Alimerka, Integrasys, Codesyntax, TreeLogic, Intercom Factory, GESIMDE, Yaco, SoftTelecom
DESAFIOS-10	MICINN	BBVA-GlobalNet, LambdaStream, Deimos Space
PROMETIDOS	Madrid Regional Government	Deimos Space, Atos Origin, BBVA-GlobalNet, Thales, Telefónica I+D
MTECTEST	Madrid Regional Government	Deimos Space
SEIF awards	Microsoft SEIF	Microsoft Research
PhD Scholarships	Microsoft	Microsoft Research
ENTRA	FP7: STREP	XMOS
VARIES	FP7: ARTEMIS	Barco NV, HI iberia, IntegraSys, Tecnalia, Sirris, Spicer, Fraunhofer Gesellschaft, Pure-Systems Gmbh, STiftelsen Sintef, Autronica, Franders Mechatronics Technology Centre, Atego Systems, Teknologia Tutkimuskeskus VTT, Mobisoft, HIQ Finland, Softkinetic Sensors, Macq, Metso Automation.
4CaaST	FP7: IP	Telefónica I+D, SAP, France Telecom, Telecom Italia, Ericsson, Nokia-Siemens, Bull SAS, 2nd Quadrant, Flexiant
POLCA	FP7: STReP	Maxeler, Recore
Cadence	EIT	Reply SpA
FI-PPP-Liaison	EIT	Engineering Ingegneria Informatica SpA, Orange, Thales, Create-Net
Contracts	Microsoft	Microsoft Research
Contracts	AbsInt	AbsInt GmbH
Contracts	Boeing	Boeing Research & Technology Europe
Contracts	Telefonica	Telefonica I+D
Contracts	LogicBlox	LogicBlox

Figure 2.1. Some companies with which the IMDEA Software Institute has collaborated through projects and contracts to date.

Other forms of collaboration with industry include the *industrial funding of doctoral and master students* working at the Institute on industry-relevant topics (e.g., Microsoft funds research assistants working on software verification and security), *transfer of research personnel trained at the Institute to companies* (IMDEA Software-trained personnel has already been transferred to companies such as Atos, Microsoft, Google, or Logicblox), funding by industry of *research stays of Institute researchers at company premises* (e.g., Institute researchers have made industrially-funded extended stays at Deimos Space, Microsoft Redmond in the US, or Microsoft Cambridge in the UK, and a framework agreement has been signed with Microsoft for this purpose), *access to the Institute's technology and scientific results* (e.g., researchers of the Institute have met with personnel from BBVA, Telefónica I+D, Ericsson, GMV, INDRA, IBM, Canal de Isabel II, Interligare, or Lingway, among many others, to present their main research results), access to the Institute's researchers as consultants, participation of company staff in Institute activities, etc.

2.2. Cooperation with Research Institutions

As a international research organization, the Institute collaborates with many universities and other research centers worldwide. As with companies, an important way in which such cooperation happens is through focused collaborations in the framework of *collaborative projects*, funded through competitive calls or industrial contracts. At the same time, and similarly to the industrial case, the Institute has established *longer-term, strategic partnerships* with a number of research institutions, in the Madrid region and internationally, in order to allow more strategic collaborations and reach objectives that go beyond those of individual projects. At present the Institute has active long-term agreements with the following universities and research centers:

- Universidad Politécnica de Madrid (since November 2007).
- Universidad Complutense de Madrid (since November 2007).
- Universidad Rey Juan Carlos (since January 2008).
- Roskilde University, Denmark (since June 2008).
- Consejo Superior de Investigaciones Científicas (since November 2008).
- Swiss Federal Institute of Technology (ETH) Zurich (since November 2012).
- Microsoft Research (since December 2012, with a Joint Research Center established in 2014).

These agreements establish a framework for the development of collaborations that include the joint participation in and development of graduate programs; the joint use of resources, equipment, and infrastructure; exchange of staff; joint participation in research projects; the association of researchers and research groups with the Institute; or the joint commercialization of technology. In particular, research assistants at the IMDEA Software Institute can follow graduate studies at any of the cooperating Institutions, while funded by the IMDEA Software Institute.

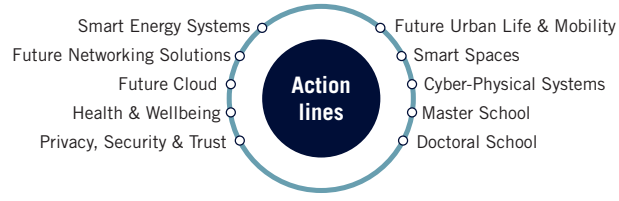
To illustrate the scope and importance for the Institute of these agreements, we offer here some highlights. The agreement with the Universidad Politécnica de Madrid (UPM) has allowed the location of the Institute building in its Montegancedo Science and Technology Park. In addition, the Institute runs jointly with UPM a graduate program, instrumented currently as a separate track on *Software Development through Rigorous Methods* in an existing Masters / PhD program at UPM ("MUSS / DSS"). Most research assistants at the IMDEA Software Institute obtain their Masters and PhD following this program, and all Institute faculty have "Venia Docendi" (i.e., can act as university faculty members) in this program. Under the agreement with the Consejo Superior de Investigaciones Científicas, two of its researchers —Cesar Sánchez and Pedro López— are full-time faculty at the Institute. Under the agreement with Roskilde University, one of its full professors —John Gallagher— is also part-time senior researcher at the Institute. As mentioned before, the agreement with ETH Zurich includes the joint development and commercialization of the ActionGUI technology, from the Institute's Modeling Lab. Finally, the Institute of course also collaborates with the other Institutes in the IMDEA network. As an example, the Insti-

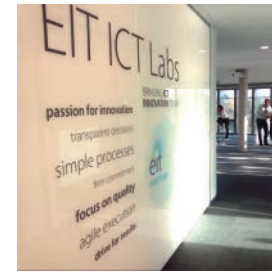
tute has secured and coordinates the AMAROUT-I and AMAROUT-II COFUND programs of Marie Curie fellowships, which fund personnel in all the IMDEA Institutes, and provides other services to the IMDEA network, including hosting a joint coordination unit.

The Institute also has a strong presence in national and international bodies. It is a member of *Informatics Europe*, the organization of all deans, chairs, and directors of the leading Departments and Institutes of Computer Science in Europe, similar to the CRA in the US. In addition, the Institute is a member of ERCIM, the *European Research Consortium for Informatics and Mathematics* through SpaRCIM, the Spanish representative in ERCIM. Manuel Hermenegildo, IMDEA Software Institute Director, is the President of the SpaRCIM Executive Board and a member of the Informatics Europe steering board.

2.3. EIT ICT Labs

In June 2013, IMDEA Software officially became an Associate Partner of EIT ICT Labs, as the first Spanish organization to enter its Pan-European network of seven full national nodes (in Helsinki, Stockholm, Berlin, London, Eindhoven, Paris, and Trento) and two associate nodes (Budapest and Madrid, located at IMDEA Software).





EIT ICT Labs is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT), which includes some of the leading educational, research and industrial actors in the ICT innovation ecosystem in Europe. Its mission is to combine the educational, research and industrial tools and activities to drive and foster ICT innovation on the European scale in the following strategic areas: Smart Energy Systems, Future Networking Solutions, Future Cloud, Health and Wellbeing, Privacy, Security and Trust, Future Urban Life and Mobility, Smart Spaces, and Cyber-Physical Systems. These areas are complemented by an integrated and innovation-driven Master and Doctoral School and a Business Development Accelerator.

One of the key goals of IMDEA Software as the Spanish Associate Member is to promote, motivate, and organize the presence of EIT ICT Labs in Spain, and to foster the evolution of the Spanish Associate Partner Group (APG) – which includes some of the most prominent players in the ICT innovation arena, such as Telefónica, Indra, Atos, the Technical University of Madrid (UPM), and the Barcelona Supercomputing Center (BSC) – towards a fully operational EIT ICT Labs node. Together with these strategic partners, the Institute is working on developing innovation-oriented projects within the framework of EIT ICT Labs, increasing its presence in Spain through interaction with regional and national governments, and boosting and creating synergy between the entrepreneurship initiatives and mechanisms led by the members of the APG and beyond.

IMDEA Software has participated in the EIT ICT Labs Business Plan for 2014 with the following activities:

- Three research and innovation activities in the fields of Privacy, Security, and Trust (project CADENCE), Cyber-Physical Systems (project cPAS), and the FI-PPP Liaison. More details are provided in Chapter 5.
- Further development of the Madrid Co-Location Center (CLC), hosted in the premises of IMDEA Software, which is the home for the EIT ICT Labs activities and the meetings of the Spanish APG. The CLC is equipped with videoconferencing equipment that allows online collaboration, ample office space and meeting facilities, office space for start-ups, and work and collaboration areas for the students in the EIT ICT Labs masters and doctoral programs.
- Development of the Madrid Business Development Accelerator (BDA) segment which is a part of the EIT ICT Labs BDA network, a group of 50 specialists helping in bringing

ideas to market and providing services such as coaching, access to finance, or soft landing, at a pan-European level. This has also included participation in and organization of events related to innovation and entrepreneurship such as, e.g., Spain Startup.

- Preparation for the launch of the EIT ICT Labs Doctoral Training Center and the Master Program in Data Analytics in 2015, in cooperation with UPM, which is a part of the EIT ICT Labs educational initiative that allows doctoral and master students to obtain not only a recognized technical education, but also entrepreneurial skills and the opportunity to work with European top research facilities and leading business partners.

Joint Research Center
institute imdea software
Microsoft Research

2.4. Microsoft Research - IMDEA Software Joint Research Center

The Microsoft Research - IMDEA Software Institute Joint Research Center (http://www.msr-imdeasw.org/) started operations in late 2013 with the objective of framing and boosting the significant research collaborations between Microsoft Research and the IMDEA Software Institute in software science and technology.

The Joint Research Center was presented officially on April 3, 2014, on the occasion of the first Microsoft Research and IMDEA Software Institute Workshop (MICW 2014), which took took place on April 2–4, 2014, at the IMDEA Software building in Madrid.

This was the first in a series of annual workshops aimed at reinforcing the collaboration between these two institutions, with researchers from both sides working together on several research topics. It was organized by Judith Bishop and Georges Gonthier from Microsoft Research and by Gilles Barthe and Manuel Hermenegildo from the IMDEA Software Institute.

These workshops bring together researchers and students to discuss their collaborative work on hot topics in software in order to advance the state of the art and, where possi-

ble, to bring those advances to market. The focus of the first workshop was on verification (coordinated by Alexey Gotsman and Francesco Logozzo), programming languages (coordinated by Pierre-Yves Strub and Georges Gonthier), and security (coordinated by Juan Caballero and Ben Livshits).

The collaborations between IMDEA Software and Microsoft involve around 30 researchers from both sides and have resulted in more than 25 publications in top-level venues to date, including for example four joint papers at the top-ranked ACM Symposium on Principles of Programming Languages (POPL), in 2014.

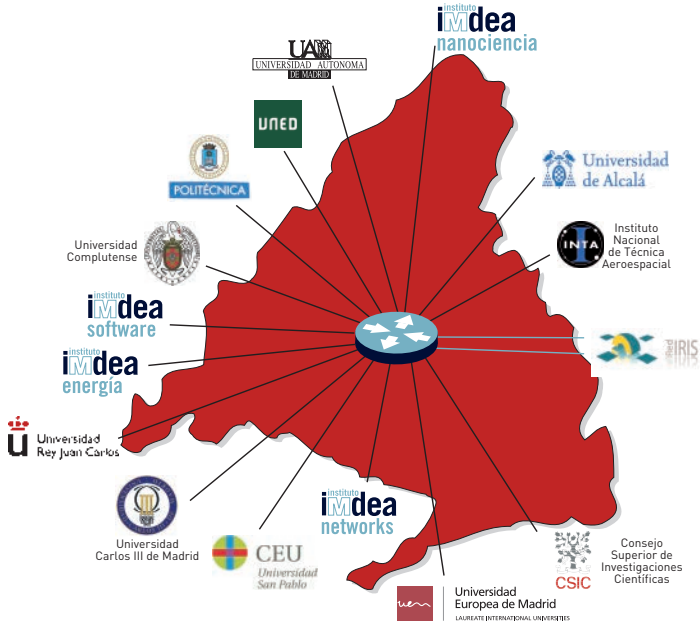
2.5. Telefónica - IMDEA Software Joint Research Unit

Through the Joint Research Unit, IMDEA Software and Telefónica I+D cooperate on developing software architectures and high-level components within the framework of the FI-WARE initiative. This cooperation has been developing since 2012. The Joint Research Unit works on different topics, such as brokerage in the context of Internet of Things (IoT), and facilitating the definition and automatic deployment of cloud application components. In 2014, the Joint Research Unit has been expanded with an expert on IoT component controllers and brokers, and is active within the ongoing Phase 3 of the FI-PPP Program. The Joint Research Unit also organizes education activities in the area of FI-WARE technology.

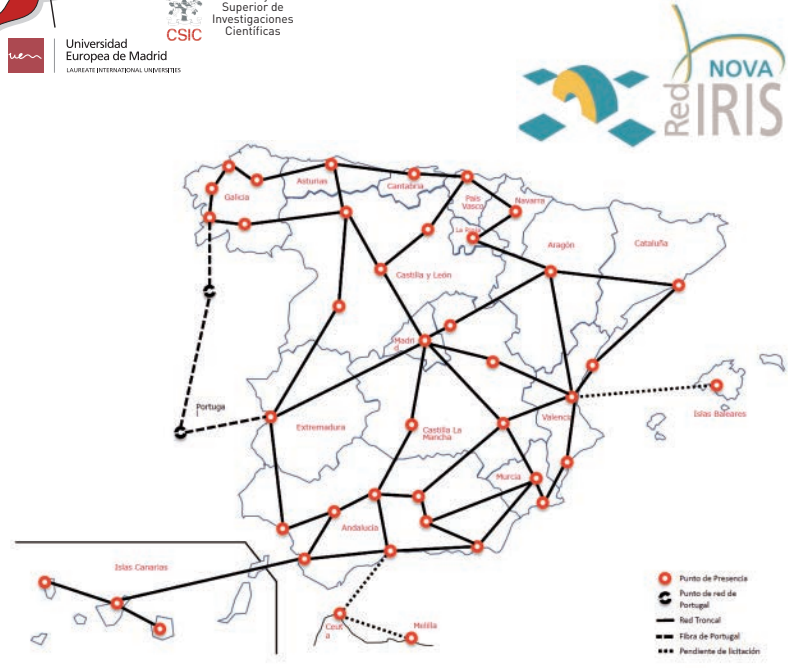
2.6. REDIMadrid

The IMDEA Software Institute manages the academic and research Internet backbone of the Madrid Region, *REDIMadrid*, funded by the Madrid Regional Government, which currently provides high-speed connections at up to 10 Gbps to the universities and research institutes located in the Madrid region (including IMDEA Software and the other IMDEA institutes).

REDIMadrid



The IMDEA Software Institute also hosts and operates the new *EIT ICT Labs node* of the Madrid and Spanish networks, located at the EIT ICT Labs Madrid Co-location Center and provided jointly by the Spanish High-speed Research Network Backbone, *RedIRIS-NOVA*, and *REDIMadrid*. This link is available as an experimentation infrastructure and can support speeds of up to 100Gb. This recent expansion of RedIRIS-NOVA and REDIMadrid has been funded jointly by the Spanish and Madrid Governments in direct support of the EIT ICT Labs associate partner group in Spain.



research

3.1. "Greener" Software: Verifying and Controlling Resource Consumption [25]

3.2. Formal Verification of Cyber-Physical Systems [27]

3.3. Architecture-Driven Verification: Tackling The Complexity Of Modern Software [28]

3.4. Digital privacy [29]

3.5. Fighting Malware in Cybercrime & Targeted Attacks [30]

3.6. Cryptography for Next Generation Cloud Computing [32]

3.7. Model-Driven Data Security and Privacy Management [33]

3.8. Concurrent Software Reliability [34]

3.9. Automated Software Testing and Failure Recovery [36]

annual report

2014

The research activities carried out by the IMDEA Software Institute address directly its core mission: to advance the scientific and technological foundations that will allow the cost-efficient development of software characterized by sophisticated functionality and high quality, in terms of safety, reliability, and efficiency.

This chapter describes the key lines of research currently pursued by the scientists of IMDEA Software. A common characteristic of all these lines is the attention to two tightly interrelated aspects: on one hand the development of sound and mathematically rigorous *foundations* which are at the same time oriented towards solving practical problems. On the other hand, the development of well-founded and cost-effective *tools and prototypes*, which are fundamental to both experimentation and technology transfer towards integrated production-grade systems.

3.1. "Greener" Software: Verifying and Controlling Resource Consumption

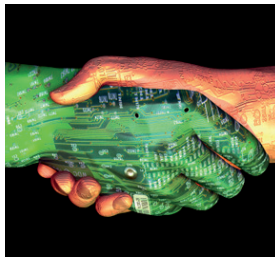
Energy consumption and the environmental impact of computing technologies is a major worldwide concern. It is a significant issue in systems ranging from energy-hungry server farms to billions of frequently charged smartphones, tablets, smart watches, and sensors. As a result of the huge growth in cloud computing, Internet traffic, high-performance computing, and distributed applications, current data centers consume very large amounts of energy, not only to process and transport data, but also for cooling. There is also a need for improving the battery life of increasingly complex portable devices, including, e.g., implantable medical devices.

In spite of the recent rapid advances in power-efficient hardware, most of the potential energy savings are wasted by software that does not exploit these hardware energy-saving

features and performs poor dynamic management of tasks and resources. To face this challenge, researchers at the IMDEA Software Institute are promoting energy efficiency to a first-class goal in software design, and developing tools that facilitate the production of "greener" devices, i.e., devices that make a certifiably more efficient use of their available energy and, in general, of *resources* (e.g., execution time or memory, as well as other user-defined resources like network accesses or transactions).

IMDEA Software researchers have developed novel automatic techniques for resource usage analysis, verification, debugging, and optimization, which are based on the sound and practical framework of abstract-interpretation. These techniques are implemented and integrated into IMDEA's state-of-the-art tools, which are aimed at helping software engineers develop energy-efficient code and systems. In particular, the pioneering CiaoPP system provides a general framework for predicting with high confidence the resources consumed by a given piece of software and for debugging/certifying such consumption with respect to specifications. The tool is highly adaptable to different languages, hardware, and resources because it is built around a customizable static analyzer with a versatile assertion language. It can help programmers significantly reduce resource usage of programs, including their energy use and/or total execution time. This results in significant improvements in battery life (e.g., in smart phones and other small devices), or reductions in electricity consumption (e.g., at data centers).

These tools are developed in collaboration with industry, and applied to concrete examples extracted from industrial application code. In particular, a part of this research on "greener software" is being performed within the European project ENTRA (see Chapters 5 and 7).



3.2. Formal Verification of Cyber-Physical Systems

Modern computers are not standalone devices sitting on our desktops, but are increasingly seen embedded in everyday devices, systems and structures such as smart phones, buildings, medical devices and automobiles. The drastic reduction in the cost of sensing, actuating, computing and communication technology has enabled the proliferation of a new genre of engineered systems, referred to as Cyber-Physical Systems (CPS), in which networked embedded processors interact tightly with a physical environment to achieve global complex functionalities.

Cyber-physical systems will be a key enabling technology of the future in tackling societal and economic challenges arising in areas such as manufacturing, communication, infrastructure, energy, health-care, and transportation. Hence, governments around the world including the United States and the European Union have established several funding initiatives to exploit this potential. Cyber-physical systems invariably manifest in safety-critical domains—such as automotive, aerospace and medical devices—so ensuring reliable performance is of utmost importance. However, the state-of-the-art techniques fall short in guaranteeing correct behavior, as is evident from the recent episodes of software recalls in the automotive and medical devices industries to fix bugs. Therefore, the grand research challenge is to build techniques for the development of high-confidence cyber-physical systems.

While formal methods have been successfully applied to the analysis of stand-alone hardware and software, CPS differ from traditional software in the tight interactions with the physical system it controls, and in that CPS run on one or more embedded processors which communicate with each other. Hence, CPS are hybrid systems that encompass both discrete and continuous behaviors owing to the digital components and the physical environments, respectively. The central scientific challenge in CPS formal verification lies in dealing with this unprecedented complexity arising due to the tight coupling of computation, control, and communication.

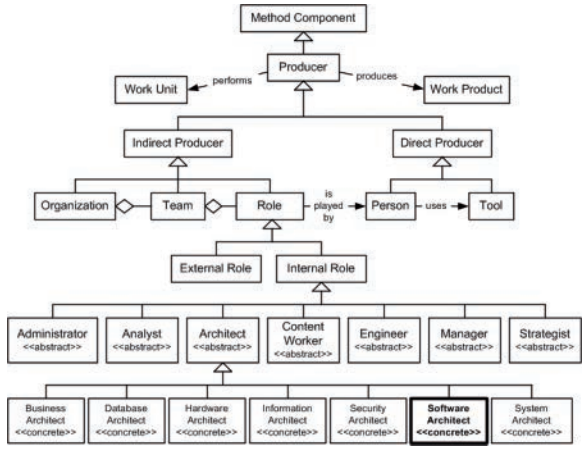
Researchers at the IMDEA Software Institute are actively involved in this exciting new area by focusing on the development of the state-of-the-art technology for verification of cyber-physical systems, particularly, in the early design phase, where reliability has a huge impact on the development cost of the products. The research carried out at IMDEA Software addresses the scalability of current verification techniques by designing novel state-space reduction algorithms and tools. Given the inter-disciplinary nature of the area, this scientific endeavor is carried out in collaboration with experts in control theory, dynamical systems, and formal methods from several institutes and universities in the US and Europe.

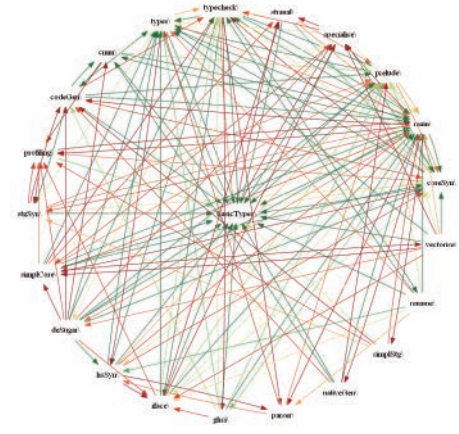
3.3. Architecture-Driven Verification: Tackling the Complexity of Modern Software

While the modern information society critically relies on software systems, with some of its most vital processes controlled by software, at the same time software is notoriously unreliable. This is a consequence of a systemic problem, and, given the current trends in software development, in the future the cost and dependability problems will only be exacerbated. The growing dependence of modern society on software systems makes this situation unsustainable.

Software verification has the potential to resolve this problem: its goal is to ensure the correctness of software by proving that it satisfies a given property in *all* possible situations. Formerly a purely theoretical area, since the year 2000 software verification has experienced a resurgence of interest from practitioners and is now emerging as a cutting-edge approach to improving software quality. Although there is much excitement in the verification area, there is still a huge distance to go before we will be able to verify pieces of software as complex as a modern operating system kernel. This is because the cost-benefit ratio of current verification technology is not good enough to scale it to major software systems. Software verification is currently good at dealing with programs that are either big, but simple, or complicated, but small. Unfortunately, modern software is both big and complicated. IMDEA Software Institute researchers are developing radically new verification methods aiming to overcome this problem.

The hypothesis underlying this research line is that the main reason for the inadequacy of the existing verification approaches when dealing with complex software is their generality. The techniques they suggest are based on generic principles that come from properties of programming languages, which allows applying such techniques to arbitrary programs. However, since they cannot take advantage of the particular ways in which programs are usually written in those languages, they require too much labor





and do not scale to big and complicated systems. At the IMDEA Software Institute, we are developing methods and tools for cost-effective verification of real-world systems software by exploiting the way programmers write it: in practice, they stick to informally described patterns, idioms, abstractions and other forms of structure contained in their software, which are together called its *architecture*. IMDEA researchers harness this trend to develop verification methods and tools that are tailored to the architectures used in modern systems software.

3.4. Digital Privacy

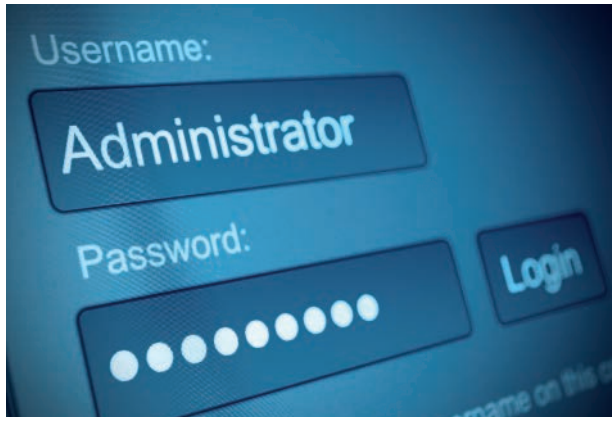
Much of our most private data is collected permanently (for instance through web browsing or networked devices that we carry with us), sent over the air to external third parties, stored in the cloud and redistributed (at best in aggregated form) to other third parties. While the availability of this data opens up tremendous opportunities for society, the economy, and individuals, it also exposes users to potential attacks against their privacy. For the information society to thrive, we need to protect ourselves against such attacks. Unfortunately, our privacy is typically in conflict with requirements on functionality, performance, usability, and cost:

- The release of sensitive information such as medical records, smart-metering data, or browsing habits severely threatens the privacy of users. However, society and the economy benefit from utilizing this data, for example, for computing health statistics, for offering competitive pricing, or for targeted advertisement.

- Mechanisms such as encryption can be used for hiding the content of messages that are exchanged between users. However, without incurring significant traffic overhead, they typically cannot hide features such as the size of the content or the mere fact that a message has been exchanged.

- Techniques such as caching greatly improve the browsing experience by increasing the responsiveness of web browsers. However, they also introduce variations into the response times of requests, which can be observed and exploited to recover private information about users.

In the presence of such conflicting requirements, perfect privacy is impossible or simply too expensive to achieve. Rather, the challenge is to identify trade-offs in which systems meet their requirements and at the same time protect the privacy of their users to a sufficient degree.



Researchers at the IMDEA Software Institute are working on the next generation of tools for ensuring the privacy of real systems. The first research thrust is to develop meaningful measures and metrics of privacy that allow users and analysts to agree on what it means for data to be "sufficiently" protected. The second research thrust is to develop tools that enable guaranteeing that the deployed systems comply with this degree of protection. A key requirement of these approaches is that they enforce privacy preventively, that is, before the program is deployed and under attack.

Emblematic applications that have been developed at the IMDEA Software Institute are a tool that ensures the privacy of smart metering protocols, while at the same time allowing for relevant information to be extracted, and a tool that enables quantifying the information leaked by features of web-browsing traffic.

3.5. Fighting Cybercrime and Targeted Attacks

Cyberattacks have become a huge challenge to developed societies. Two main threats dominate this environment: *cybercrime* and *targeted attacks*. Cybercriminals compromise large numbers of Internet-connected hosts, and develop ways for monetizing those compromised hosts and their users. They focus on economies of scale; for them, any compromised host has some, even if low, value. Even if the value of each target is low, their large number makes the profit worth. Compromised hosts are valued for the user data they hold or as assets. Those assets can be used (or bought and sold) to launch malicious activities such as sending spam, launching denial-of-service (DoS) attacks, mining virtual currencies (i.e., Bitcoins), faking user clicks on online advertisements (i.e., click-fraud), or simply as stepping stones to hide the attacker's real location. Users of compromised hosts can be phished to steal their credentials and can be convinced to buy licenses of rogue software.

Targeted attacks differ from cybercrime in that they focus on high-value targets. Targeted attacks have become a focus of the security industry, which has coined a new term for them: *Advanced Persistent Threats* (APTs) that refers to highly determined, well-funded, cyber-attackers, who persistently target an individual, a group, or an infrastructure. High-value targets include politicians, journalists, activists, enterprises, and critical infrastructures.

Two components are at the core of both cybercrime and targeted attacks. The first key component are malicious programs (i.e., malware) that the attacker installs on Internet-connected computers without the owner's informed consent. Malware includes bots, viruses, RATs, trojans, rootkits, fake software, and spyware. Malware enables attackers to establish a permanent presence in a compromised computer and to leverage that computer for their nefarious goals.

The second key component are malicious servers, geographically distributed across the Internet, which attackers use to control the malware (e.g., send instructions) and to collect data exfiltrated from the compromised hosts. In recent years, attackers have started to take advantage of a booming cloud hosting services market where hosting is cheap, easy to contract, servers can be rented in multiple geographic locations, short leases are available, and payment is based on resources consumed. These enable attackers to build large, highly dynamic, malicious server infrastructures, while minimizing the investment loss if a malicious server is taken down.

Researchers at the IMDEA Software Institute are developing novel defenses against malware-based operations including techniques for detecting the malicious server infrastructures they rely on. This research is being performed in part within the MALICIA and CADENCE projects (see Chapter 5).

3.6. Cryptography for Next Generation Cloud Computing

Cloud computing is a fast growing paradigm in which users lease computation resources from powerful service providers. Virtual machines, remote storage, email, web-content, databases are only some examples of services that are nowadays outsourced to the Cloud. This paradigm is very appealing to individuals and businesses due to its significant benefits: reduced IT costs, increased mobile productivity, convenient access to remote resources from multiple devices, different geographic locations, etc. The downside of cloud computing is that keeping a clear control over the data and the computations that are outsourced to the Cloud is becoming more difficult. This new working scenario exposes users to faults and attacks that are out of the control of users and can seriously threaten privacy and integrity of data and computations delegated to the Cloud. As an example, if the cloud provider falls under an attack, this may cause the tampering or the leakage of sensitive users data (such as credit card information or medical records) with devastating consequences.

To address these issues, researchers at the IMDEA Software Institute are working on securing the next-generation cloud infrastructure in such a way that users will be able to outsource their data and computations to untrusted providers in a fully reliable manner. The main goal of this research is to protect cloud users with respect to privacy and integrity. For privacy, cloud providers should be able to perform the operations delegated by the users without learning any unauthorized information about the users data. Importantly, such strong form of privacy also prevents any attacker that would penetrate into the Cloud system from learning the content of the data therein stored. For integrity, the key idea is to enable users to verify that cloud providers have indeed operated correctly (for example, to check that the original data has not been modified without the user's authorization) without, however, spending too many resources to perform this check.

To achieve these goals, our research builds on cryptography – the science of developing methods for protecting information and communication against misbehaving parties. While initially focused on encrypted communications in the military or diplomatic domain, modern cryptography has expanded considerably and already plays a central role in the Internet. To play a similar role in the Cloud, one must design new, advanced, cryptographic mechanisms that can address privacy and integrity in this new scenario. Homomorphic encryption, verifiable computation protocols, and zero-knowledge proofs are some examples of cryptographic primitives useful in this context.

Researchers at the IMDEA Software Institute are therefore investigating novel cryptographic techniques that can achieve these advanced functionalities so that users will be able to outsource data and computations to the Cloud, and at the same time not to risk for their privacy and integrity.

3.7. Model-Driven Data Security and Privacy Management

The derivation of code from models (model-driven software development) offers the advantage of automating the coding of at least certain parts of applications, an approach which can avoid the introduction of errors that is frequent in manual software production. IMDEA Software researchers are applying this methodology to the problem of semi-automatic development of data-management applications that have strict security and privacy requirements.

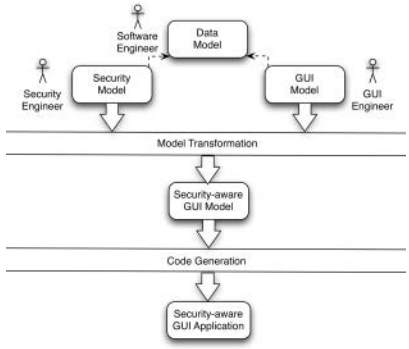
Data-management systems are focused around so-called CRUD actions that create, read, update, and delete data from persistent storage. These actions are the building blocks for numerous applications, for example dynamic websites where users create accounts, store and update information, and receive customized views based on their stored data. When the data managed is sensitive, then security is a concern and the use of these actions must be controlled.

Researchers at the IMDEA Software Institute, in collaboration with ETH Zurich, have developed a novel model-driven methodology for developing secure data-management applications. System developers proceed by modeling three different views of the desired application: its data model, security model, and GUI model. These models formalize respectively the application's data domain, authorization policy, and its graphical interface together with the application's behavior. Afterwards a model-transformation function lifts the policy specified by the security model to the GUI model. This allows a *separation of concerns* where behavior and security are specified separately, and subsequently combined to generate a security-aware GUI model. We have also implemented a toolkit, called ActionGUI, which performs the aforementioned model transformation and, from the resulting security-aware GUI model, generates a deployable application, along with all support for access control. In particular, when the security-aware GUI model contains only calls to execute CRUD actions, then ActionGUI will generate the complete implementation automatically. Since experience shows that it is easy to make logical errors and omissions in the models, we have also developed tools for analyzing non-trivial properties of the data, security, and GUI source models, in a way that is mathematically rigorous and automated.

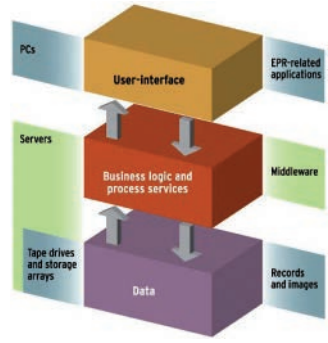
IMDEA Software researchers have also developed applications that provide evidence of the applicability of ActionGUI, including a web application for managing eHealth records. The access-control policy regulates, in particular, the access to the patients' highly sensitive records.

Motivated by the increasing concerns of both users and regulators about privacy breaches in data-management applications, interest is now focused on extending ActionGUI to include *privacy models* as primary artifacts in the model-driven software development

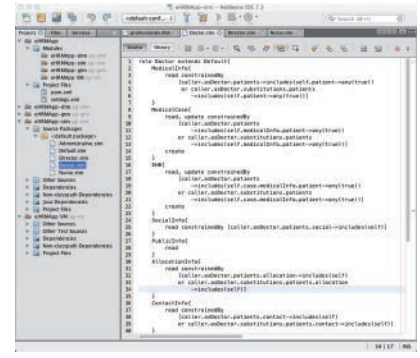
process. Although related to security modeling, privacy modeling differs substantially as it requires modeling privacy-related notions that are not part of standard security modeling languages. In particular, it must deal with policies that enable users to define: (i) the data that shall be accessible only upon the user's explicit *consent*; (ii) the specific *purpose* that shall be pursued when accessing the user's sensitive data; and (iii) the specific circumstances that shall trigger an immediate privacy *notification* to the user.



Model-driven development of security-aware GUIs.



3-tier architecture



ActionGUI: An example of a security model (screenshot)

3.8. Concurrent Software Reliability

The importance of software reliability has dramatically increased due to the popularization of concurrent software. Software has become inherently concurrent due, on one hand, to the need to optimize the use of new multi-core and multi-processor hardware, and on the other hand, because many systems are increasingly distributed and must

Satellites have to be autonomous up to a certain degree. The programs running in their computers continuously monitor for deviations from their scheduled trajectories and take the appropriate decisions to correct them.

respond to humans in a timely manner. This distribution is present at a small scale, for example inside our mobile phones, or at internet scale, for example in social networks and planet-wide information systems. Consequently, this software differs from classical approaches to concurrent programming in crucial aspects, like the structure of the synchronization—where large blocks are avioded by using fine-grain or lock-free algorithms—or the use of asynchronous programming primitives.

Testing or reasoning about modern concurrent systems requires considering a large number of simultaneous interactions between the constituent components. This complexity makes testing less effective and leaves verification as a more appealing technique for software reliability.

In order to face the challenges of reliability of modern concurrent software, we need to develop new verification methods, both for specifying and assessing the correctness of concurrent programs. First, formal verification requires a description of those aspects of the behavior of a given software system that are considered crucial. New specification languages must provide this description in a way that is humanly usable and computationally tractable. Second, automatic verification techniques are desirable because they do not require human ingenuity and intervention, and can be applied to existing software. It is a big challenge to design automatic techniques that tackle concurrent software of realistic sizes. Alternatively, deductive techniques can handle sophisticated cases but at the cost of a higher human intervention. The challenge with deductive techniques is to increase their automation and reduce the expertise necessary to use them.

Researchers at the IMDEA Software Institute are involved in the pursuit of novel automatic and semi-automatic software verification techniques, and richer specification logics for concurrent and reactive software. These techniques are aimed at a wide range of aspects of modern concurrent software: asynchronous program verification, fine-grain and lock free algorithms, concurrent data-types, refinement of concurrent object-oriented programs. This research line includes not only foundational research but also the development of verification tools, for example for the analysis of asynchronous concurrent software and for the deductive verification of concurrent fine-grained data-types.



3.9. Automated Software Testing and Failure Recovery

In addition to being complex, modern software poses the additional challenge that its structure evolves and often deteriorates as it grows, and it is usually unfeasible to estimate during the development phase how external factors in the execution environment will impact its behavior. This leads to faults that are difficult to anticipate. It is necessary to detect as many of these faults as possible before releasing a software artifact. However, since the complete elimination of faults is not always possible or economically feasible, it is also useful to instantiate techniques that can mitigate the effects of previously undetected faults while the software system is running.

The predominant industrial approach to achieving software reliability is testing, in which a piece of software is exercised repeatedly trying to gain confidence that the software behaves as intended. Software testing is typically embedded in the software development life cycle to expose faults before deployment. Testing is an alternative and complementary approach to verification, which typically requires higher human expertise and is less automated. While it cannot cover all scenarios, testing is readily applicable both for small and large systems. Designing, implementing, and running tests, though, can still be very expensive. The cost of software quality assurance activities, in general, often exceeds half the overall cost of software development and maintenance. It is therefore essential to find the right balance between cost and effectiveness of quality assurance techniques.

Researchers at the IMDEA Software Institute work on designing testing techniques that are highly automated, and as a consequence cost effective. Such techniques can automatically identify test inputs that exercise the relevant features of a software artifact, can decide whether the execution of a test case matches the expected behavior, and can automatically evolve the produced test suites together with the evolution of the software artifact under development, thus limiting the costs of test case maintenance.

Despite the best efforts at developing effective testing and analysis techniques to detect as many faults as possible during the development phase, some faults still escape the quality control, and can ultimately affect the functionality of deployed systems. As a consequence, researchers at the IMDEA Software Institute have also been working on designing and implementing cost-effective techniques that make deployed applications more resilient to failures. Such techniques are intended to maintain a faulty application functional in the field while the developers work on more permanent fixes.

people

4.1. Faculty [40]

4.2. Postdoctoral Researchers [49]

4.3. Visiting Faculty [52]

4.4. Research Assistants [53]

4.5. Interns [57]

4.6. Project Staff - Joint Research Units [57]

4.7. Project Management and Technology Transfer Unit [58]

4.8. Technical Support and Infrastructures Unit [58]

4.9. Management and Administration [59]

annual report 2014

The IMDEA Software Institute strives towards the level of excellence and competitiveness of the highest-ranked institutions worldwide. Success in this goal can only be achieved by recruiting highly-skilled personnel for the scientific teams and support staff. The Institute considers this one of the key critical factors and measures of its success.

Competition for talent in Computer Science is extremely high at the international level, since essentially all developed countries have identified the tremendous impact that IT has on the economy and the crucial competitive advantage that attracting truly first class researchers entails. To meet this challenge, the Institute offers a world-class working environment that is competitive with similar institutions in Europe and in the US and which combines the best aspects of a university department and a research laboratory.

Hiring at the Institute follows internationally-standard open dissemination procedures with public, international calls for applications launched periodically. These calls are advertised in the appropriate scientific journals and at conferences in the area, as well as in the Institute web page and mailing lists. Appointments at (or promotion to) the Assistant Professor, Associate Professor, and Full Professor levels (i.e., tenure-track hiring, tenure, and promotion decisions) are approved by the Scientific Advisory Board. In addition to faculty positions, the Institute also has its own programs for visiting and staff researchers, post-docs, graduate scholarships, and internships. In all aspects related to human resources, the Institute follows the recommendations of the European Charter for Researchers and a Code of Conduct for their Recruitment (http://ec.europa.eu/), which it has duly signed.

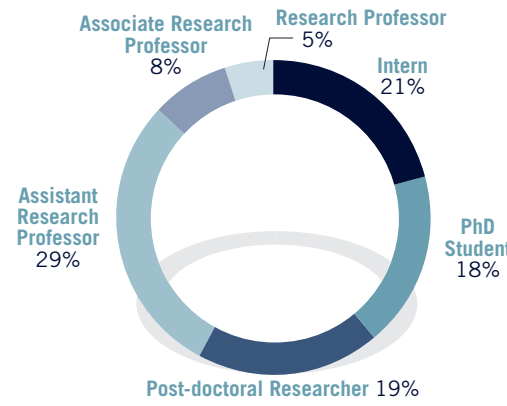


Figure 4.1. Type of position applied for.

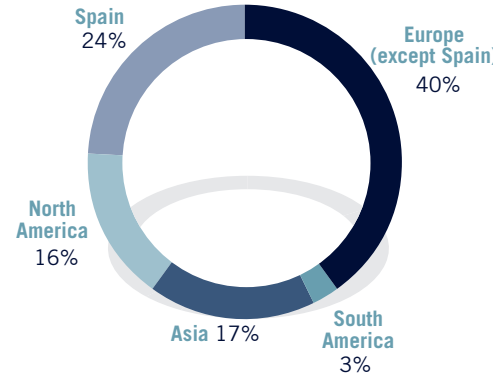


Figure 4.2. Location of previous institution for applicants at or above the postdoc level (by continent + Spain).

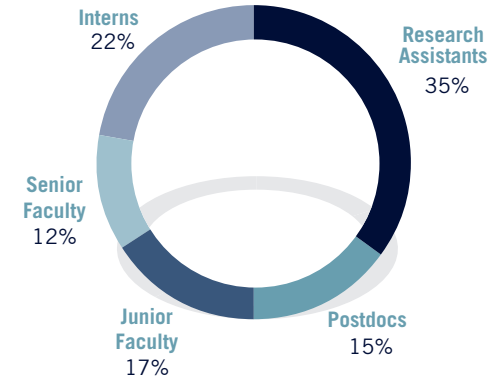


Figure 4.3. Type of position, all researchers.

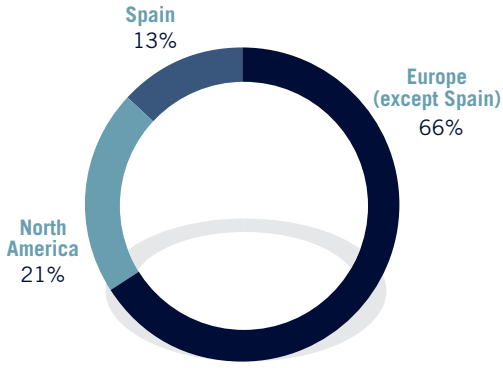


Figure 4.4. Where PhD was obtained (by continent + Spain).

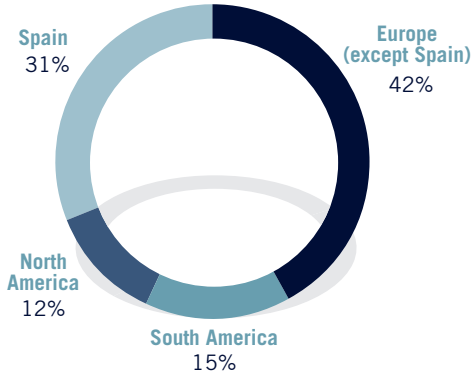


Figure 4.5. Location of previous institution, all (by continent + Spain).

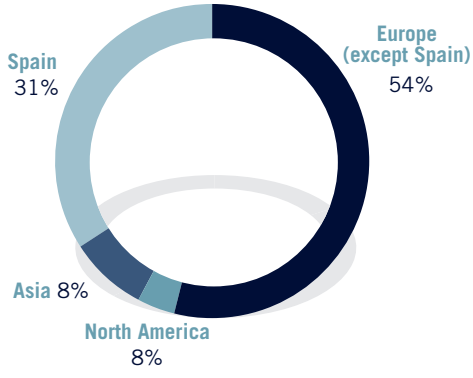


Figure 4.6. Nationality of researchers at or above postdoc level (by continent + Spain).

Applications

Figure 4.1 shows the proportions of applications received for each category during 2014: associate professors (senior researchers), assistant professors (junior researchers), postdoctoral researchers, research assistants, and interns. Figure 4.2 displays the location (by continents) of the institutions in which the applicants were at the time of application (for senior, junior, and postdoctoral positions). Spain is highlighted separately from the rest of Europe to provide a finer view of the data (level of internationalization).

Status

In 2014, the scientific staff of the Institute was composed of eight senior faculty (full or associate professors, one part-time), twelve junior faculty (tenure-track or researchers), nine postdoctoral researchers, twenty four research assistants (PhD candidates), and six project staff. Two senior faculty visitors and fifteen interns spent a variable length of time (from one month to a year) at the Institute collaborating with faculty members. Figure 4.3 shows the proportions of each category at the end of 2014 (where 33% were faculty members vs. 67% non-faculty). Figure 4.4 summarizes where these researchers obtained their PhD (by continents plus Spain), and Figure 4.5 shows the location where the Institute researchers were working previously to joining IMDEA. Finally, Figure 4.6 presents the nationalities of researchers at or above the postdoc level.

faculty

Manuel Hermenegildo

Research Professor and
Scientific Director

Manuel Hermenegildo received his Ph.D. degree in Computer Science and Engineering from the University of Texas at Austin, USA, in 1986. Since January 1, 2007 he is Full Professor and Scientific Director of the IMDEA Software Institute. He is also a full Prof. of Computer Science at the Tech. U. of Madrid, UPM. Previously to joining the IMDEA Software Institute he held the P. of Asturias Endowed Chair in Information Science and Technology at the U. of New Mexico, USA. He has also been project leader at the MCC research center and Adjunct Assoc. Prof. at the CS Department of the U. of Texas, both in Austin, Texas, USA. He has received the Julio Rey Pastor Spanish National Prize in Mathematics and Information Science and Technology and the Aritmel National prize in Computer Science, and he is an elected member of the Academia Europaea. He is also one of the most cited Spanish authors in Computer Science. He has published more than 200 refereed scientific papers and monographs and has given numerous keynotes and invited talks in major conferences in these areas. He has also been coordinator and/or principal investigator of many national and international projects, area editor of several journals, and chair and PC member of a large number of conferences. He served as General Director for the research funding unit in Spain, as well as member of the European Union's high-level advisory group in information technology (ISTAG), and of the board of directors of the Spanish Scientific Research Council and the Center for Industrial and Technological Development, among other national and international duties.

Research Interests

His areas of interest include energy-aware computing, resource / non-functional property analysis, verification, and control; global program analysis, optimization, verification, debugging; abstract interpretation; partial evaluation; parallelism and parallelizing compilers; constraint/logic/functional programming theory and implementation; abstract machines; automatic documentation tools; execution visualization; sequential and parallel computer architecture.

Manuel Carro

Associate Research Professor and Deputy Director

Manuel Carro received his Bachelor degree in Computer Science from the Technical University of Madrid (UPM), and his PhD degree from the same University in 2003. He is currently Associate Research Professor and Deputy Director at the IMDEA Software Institute, and an Associate Professor at the Technical University of Madrid. He has previously been representative of UPM at the NESSI and INES technological platforms, and is now representative of UPM at SpaRCIM and deputy representative of IMDEA Software at ERCIM and Informatics Europe. He has published over 70 papers in international conferences and journals, and received best paper awards at ICLP 2005 and ICSOC 2011. He has been organizer and PC member of many international conferences and workshops, and participated in research projects at the regional, national, and European level. He was UPM's principal investigator for the S-Cube European Network of Excellence and is currently the principal investigator of a European, a national, and a regional research project. He has completed the supervision of three PhD thesis and is actively supervising another one.

Research Interests

His interests span several topics, including the design and implementation of high-level (logic- and constraint-based) programming languages for improving the quality of software production, the analysis of service-based systems, the use of program transformation techniques for compilation on hybrid architectures, and the effective usage of formal specifications in the process of teaching programming. He has long been interested in parallel programming and parallel implementations of declarative languages, and visualization of program execution.

Gilles Barthe

Research Professor

Gilles Barthe received a Ph.D. in Mathematics from the University of Manchester, UK, in 1993, and an *Habilitation à diriger les recherches* in Computer Science from the University of Nice, France, in 2004. He joined the IMDEA Software Institute in April 2008. Previously, he was head of the Everest team on formal methods and security at INRIA Sophia-Antipolis Méditerranée, France. He also held positions at the University of Minho, Portugal; Chalmers University, Sweden; CWI, Netherlands; University of Nijmegen, Netherlands. He has published more than 100 refereed scientific papers. He was awarded the Best Paper Awards at CRYPTO 2011 and PPoPP 2013, and was an invited speaker at numerous venues, including CSF, ESORICS, ETAPS, FAST, ITP, QEST and SAS. He has been coordinator/principal investigator of many national and European projects, and served as the scientific coordinator of the FP6 FET integrated project "MOBIUS: Mobility, Ubiquity and Security" for enabling proof-carrying code for Java on mobile devices (2005-2009). He has served as PC (co-) chair of VMCAI 2010, ESOP 2011, FAST 2011, SEFM 2011 and ESSOS 2012, and been a PC member of more than 70 conferences, including CCS, CSF, EUROCRYPT, ESORICS, FM, ICALP, LICS, and POPL. He is a member of the editorial board of the Journal of Automated Reasoning and of the Journal of Computer Security.

Research Interests

Gilles' research interests include programming languages and program verification, software and system security, cryptography, formal methods and foundations of mathematics and computer science. Since joining IMDEA, his research has focused on building foundations for computer-aided cryptography and privacy and on the development of tools for proving the security of cryptographic constructions and differentially private computations.

Anindya Banerjee

Research Professor

Anindya Banerjee received his PhD from Kansas State University, USA, in 1995. After his PhD, Anindya was a postdoctoral researcher, first in the Laboratoire d'Informatique (LIX) of École Polytechnique, Paris and subsequently at the University of Aarhus. He joined the IMDEA Software Institute Institute in February 2009 as Full Professor. Immediately prior to this position, Anindya was Full Professor of Computing and Information Sciences at Kansas State University, USA. He was an Academic Visitor in the Advanced Programming Tools group, IBM T. J. Watson Research Center in 2007 and a Visiting Researcher in the Programming Languages and Methodology group at Microsoft Research in 2007–2008. He was a recipient of the Career Award of the US National Science Foundation in 2001. He is an associate editor of the journal Higher-Order and Symbolic Computation.

Research Interests

Anindya's research interests lie in language-based computer security, program analysis and verification, program logics, concurrency, programming language semantics, abstract interpretation and type systems. His primary research activities over the past couple of years have centered around automatic and interactive verification of properties of pointer-based programs and in verification of security properties of such programs.

Juan José Moreno-Navarro

Research Professor and Director for International and Industrial Relations

Juan José Moreno-Navarro received his Ph.D. degree in Computer Science from the Technical U. of Madrid (UPM), Spain in 1989. He developed a large part of his Ph.D. at RWTH Aachen (Germany). He has been Full Professor at the UPM Computer Science Department since 1996 and joined the IMDEA Software Institute upon its foundation. He served as Deputy Director up to 2008. Currently he is Director of International and Industrial Relations. He has published more than 100 papers in international conferences, books, and journals. He has organized, served in program committees, and given invited talks and tutorials in many conferences in the IST field.

He has been actively involved in research and university policy, serving as General Director for University Policies (Ministry of Education, 2009-2012), General Director for Technology Transfer and Enterprise Development (Ministry of Science and Innovation, 2009) and General Director for Planning and Coordination (Ministry of Science and Innovation, 2008-2009). During this period he has been chairman of CNEAI (Spain's Researcher Activity Evaluation Agency), has been involved in the setting up of several research infrastructures, secretary of the Spanish University Council and of the Spanish Science and Technology Council, and member of the steering board of several foundations (ANECA, UIMP, CENER-Ciemat, Universidad.es, CSIC, ISCIII, IDAE, etc.)

He has been the founding director of SpaRCIM. He has been responsible for the Spanish ICT research program, in charge on International Relations for IST, FP6 IST Committee member, and Spanish National Contact Point for the Spanish Ministry of Education and Science. Currently he is chair of the Spanish Society of Software Engineering, general chair of the Spanish Conference of Informatics 2013, and coordinator of the Spanish Turing Year.

Research Interests

His research interests include all aspects related to declarative and rigorous software development technologies. This includes software development techniques, specially specification languages, automatic generation of code (programming from specifications), and software services description. His interests also include the integration of functional and logic programming. He has led the design and implementation of the language BABEL and took part in the activities of the international committee involved in the design of the language Curry. He is also currently involved in scientific policy analysis, bibliometry, and research impact evaluation and analysis.

John Gallagher

Research Professor
(part-time)

John Gallagher received the B.A. (Mathematics with Philosophy) and Ph.D. (Computer Science) degrees from Trinity College Dublin in 1976 and 1983 respectively. He held a research assistantship in Trinity College (1983-4), and post-doc appointments at the Weizmann Institute of Science, Israel (1987-1989) and Katholieke Universiteit Leuven, Belgium (1989). From 1984-1987 he was employed in research and development in a software company in Hamburg, Germany. Between 1990 and 2002 he was a lecturer and later senior lecturer at the University of Bristol, UK. Since 2002 he has been a professor at the University of Roskilde, Denmark in the research group Programming, Logic and Intelligent Systems and the interdisciplinary Experience Lab and holds a dual appointment at the IMDEA Software Institute since February 2007. He is an area editor for the journal Theory and Practice of Logic Programming and has served on the program committee of approximately 60 international conferences, the executive committee of the Association for Logic Programming and the steering committee of the ACM SIGPLAN workshop on Partial Evaluation and Program Manipulation. He has published approximately 60 peer-reviewed papers which have over 2000 citations.

Research Interests

His research interests focus on program transformation and generation, constraint logic programming, rewrite systems, software verification, temporal logics, semantics-based emulation of languages and systems, analysis and verification of energy consumption and other properties of programs, and has participated in and led a number of national and European research projects on these topics. He is the scientific coordinator of the EU FET project ENTRA.

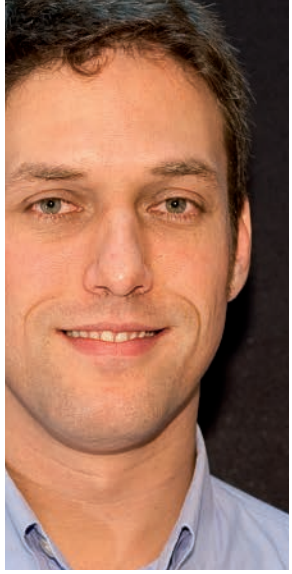
Manuel Clavel

Associate Research Professor

Manuel Clavel received his Bachelor's degree in Philosophy from the Universidad de Navarra in 1992, and his Ph.D. from the same university in 1998. Currently, he is an Associate Research Professor at the IMDEA Software Institute, as well as an Associate Professor at the Universidad Complutense de Madrid (on leave). He was Deputy Director of IMDEA Software from 2008 until April 2011. During his doctoral studies, he was an International Fellow at the Computer Science Laboratory of SRI International (1994 - 1997) and a Visiting Scholar at the Computer Science Department of Stanford University (1995 - 1997). His Ph.D. dissertation was published by the Center for the Study of Language and Information at Stanford University. Since then, he has published over 40 refereed scientific papers. He has also been involved in the supervision of 3 Ph.D. students (1 completed).

Research Interests

His research focuses on rigorous, tool-supported model-driven software development, including: modeling languages, model transformation, model quality assurance, and code-generation. Related interests include specification languages, automated deduction, and theorem proving.



César Sánchez

Associate Research Professor

César Sánchez received his Ph.D. degree in Computer Science from Stanford University, USA, in 2007, studying applications of formal methods for guaranteeing deadlock-freedom in distributed algorithms. After a post-doc at the University of California at Santa Cruz, USA, César joined the IMDEA Software Institute in 2008, becoming also a Scientific Researcher at the Spanish Council for Scientific Research (CSIC) in 2009. In 2013 he was promoted to Associate Professor at the IMDEA Software Institute. César holds a degree in Ingeniería de Telecomunicación (MSEE) from the Technical University of Madrid (UPM), Spain, in 1998. Funded by a Fellowship from La Caixa, he moved to Stanford University, USA, receiving a M.Sc. in Computer Science in 2001, specializing in Software Theory and Theoretical Computer Science. César is a recipient of the 2006 ACM Frank Anger Memorial Award. He keeps active collaborations with research groups in the USA and Europe.

Research Interests

César's general research interest are based on applications of logic for the development, understanding and verification of computational devices. In particular, formal methods for reactive systems with emphasis on the development and verification of concurrent, embedded and distributed systems. His foundational research includes the temporal verification of concurrent datatypes, runtime verification, and rich specification languages extending temporal logics.

Pierre Ganty

Assistant Research Professor

Pierre is a junior researcher at the IMDEA Software Institute since the Fall 2009. He holds a joint PhD degree in Computer Science from the University of Brussels, Belgium and from the University of Genova, Italy that he obtained late 2007. Before joining the institute, Pierre did a nearly two year postdoc at the University of California, Los Angeles (UCLA). He is the author of over 30 publications including seven journal and nineteen conference papers published in prestigious venues and accumulating close to four hundreds citations. Between 2011 and 2013 he led a Spanish national project (Paran'10) on the verification of parameterized systems. He is currently supervising one PhD thesis and has supervised eleven internships since he joined the Institute.

Research Interests

Pierre's research is about the algorithmic analysis of systems with infinitely many states, that is, the ability by a computer program to determine whether or not a given computing system (with possibly infinitely many states) comply with a given property. This is a problem of practical importance when computers are allowed to make critical decisions like how to drive cars on the roads, or medical instruments into patients. Pierre's contributions range from theoretical results all the way down to implementation of analysis algorithms.

Aleks Nanevski

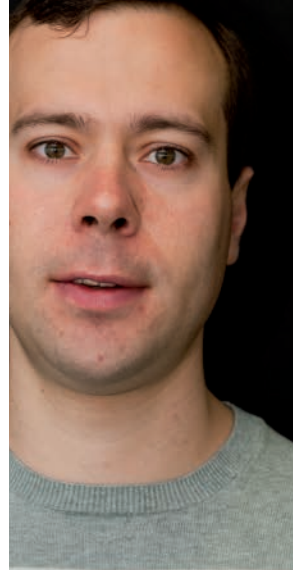
Assistant Research Professor

Aleks Nanevski obtained his PhD in Computer Science from Carnegie Mellon University, and has been a postdoctoral researcher at Harvard University and Microsoft Research in Cambridge, before joining IMDEA Software Institute in Madrid as an Assistant Research Professor. He is a recipient of Siebel Scholarship in 2004, and of Ramon y Cajal Award in 2010.

Research Interests

Aleks' research interest is in the design and implementation of programming languages and logics for software verification. More specifically, he is interested in applying programming methodology to facilitate the construction of formal proofs in mathematics in general, and of program correctness in particular.

His recent focus has been on developing the idea of structured proving. Structured proving builds on the philosophy of structured programming, to identify often used but arguably harmful linguistic abstractions of the existing logics for reasoning about programs with pointers, information flow, concurrency, etc. Such abstractions should be replaced with better ones that provide formal mathematical proofs with more structure, and thus improve on the proof's elegance, readability, development time and maintainability.



Alexey Gotsman

Assistant Research Professor

Alexey Gotsman received his Ph.D. degree in Computer Science from University of Cambridge, UK in 2009. During his Ph.D. studies, Alexey interned at Microsoft Research Cambridge, UK and Cadence Berkeley Labs, USA. He was a postdoctoral fellow at Cambridge before joining IMDEA in September 2010. Prior to his Ph.D., Alexey did his undergraduate and master studies in Applied Mathematics at Dnepropetrovsk National University, Ukraine, interning at the University of Trento, Italy in the process. He has received the prestigious Microsoft Research SEIF award to work on specifying and validating components on memory models of mobile platforms.

Research Interests

Alexey's research interests are in software verification, with particular focus on concurrent systems software. He is interested in developing both logics for reasoning about programs and automatic tools for verifying them.

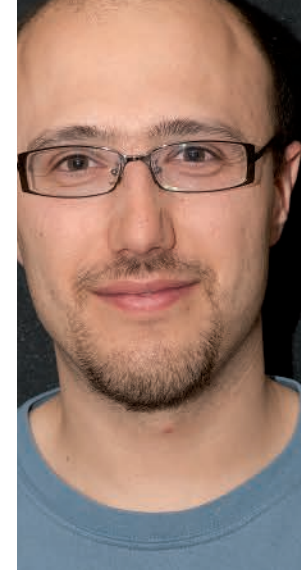
Boris Köpf

Assistant Research Professor

Boris joined the IMDEA Software Institute in September 2010 after completing a post-doc at the Max Planck Institute for Software Systems (MPI-SWS). He received a Ph.D. degree from ETH Zurich in 2007, investigating formal methods for countering side-channel attacks. Before that, he studied mathematics at the Universidad de Chile, the Universidade Federal de Campinas, and the University of Konstanz, from which he received a M.Sc. degree. He is an alumnus of the German National Academic Foundation.

Research Interests

Boris' research focuses on the foundations of computer security. In particular, he is interested in quantitative notions of security, and in techniques for computing corresponding guarantees for real systems. He applies his research to the analysis of side-channel attacks (and countermeasures) and to privacy-preserving data publishing.



Juan Caballero

Assistant Research Professor

Juan Caballero joined the IMDEA Software Institute as an Assistant Research Professor in November 2010, after receiving his Ph.D degree in Electrical and Computer Engineering from Carnegie Mellon University, USA. Prior to joining the IMDEA Software Institute, Juan was a visiting graduate student researcher at University of California, Berkeley for two years. He was awarded the La Caixa fellowship for graduate studies in 2003. Juan also holds a M.Sc. in Electrical Engineering from the Royal Institute of Technology (KTH), Sweden, and a Telecommunications Engineer degree from the Technical University of Madrid (UPM), Spain.

Research Interests

Juan's research focuses on computer security, including security issues in systems, software, and networks. He designs program analysis techniques that work directly on program binaries and applies them for finding vulnerabilities in benign programs and for analyzing malware. He also investigates the cybercrime ecosystem, machine learning applications to security, computer and network forensics, and how to build secure software.

Pavithra Prabhakar

Assistant Research Professor

Pavithra Prabhakar obtained her doctorate in Computer Science from the University of Illinois at Urbana-Champaign in 2011, from where she also obtained a masters in Applied Mathematics. She has a masters degree in Computer Science from the Indian Institute of Science, Bangalore and a bachelors degree from the National Institute of Technology, Warangal, in India. She has been on the faculty of IMDEA Software since 2011, and spent the year between 2011-2012 at the California Institute of Technology as a CMI (Center for Mathematics of Information) fellow on leave of absence from IMDEA. She is the recipient of the Sohaib and Sara Abbasi fellowship from the University of Illinois and M.N.S Swamy medal from the Indian Institute of Science for the best master's thesis. Her paper at the ACM Hybrid Systems: Computation and Control Conference 2012 received an honorable mention best paper award. She has also received a Marie Curie Career Integration Grant from the EU FP7 program.

Research Interests

Pavithra's main research interest is in the formal analysis of cyber-physical systems (CPS). Her research is at the intersection of formal methods, hybrid dynamical systems and control theory with applications in robotics and aeronautics. Her research aims at developing scalable methods for automated verification and synthesis of CPS. Her research focuses on both foundational and practical aspects, and involves building software tools for analysis of CPS.

Dario Fiore

Assistant Research Professor

Dario received his Ph.D. degree in Computer Science from the University of Catania, Italy in 2010. Prior to joining the IMDEA Software Institute in November 2013, Dario held postdoctoral positions at Max Planck Institute for Software Systems (Germany), New York University (USA), and École Normale Supérieure (France). During his PhD, he was also a visiting student at the IBM T.J. Watson research center and the New York University (USA).

Research Interests

Dario's research interests are in Cryptography and Security. He works mainly on designing provably-secure cryptographic primitives and protocols, with a particular emphasis on the security of Cloud computing applications. More specifically, some of the topics he works on include: secure delegation of data and computation to the Cloud, homomorphic authenticators, zero-knowledge proof systems, functional encryption, homomorphic encryption, and foundations of cryptography.

Alessandra Gorla

Assistant Research Professor

Alessandra Gorla received her Bachelor's and Master's degrees in computer science from the University of Milano-Bicocca in Italy. She completed her Ph.D. in informatics at the Universita' della Svizzera Italiana in Lugano, Switzerland in 2011. In her Ph.D. thesis she defined and developed the notion of Automatic Workarounds, a self-healing technique to recover Web applications from field failures, a work for which she received the Fritz Kutter Award for the best industry related Ph.D. thesis in computer science in Switzerland. Before joining the IMDEA Software Institute in December 2014, she was a postdoctoral researcher in the software engineering group at Saarland University in Germany. During her postdoc, she has also been a visiting researcher at Google in Mountain View.

Research Interests

Alessandra's research interests are in software engineering, and in particular on testing and analysis techniques to improve the reliability and security of software systems. She is also interested in malware detection for mobile applications.

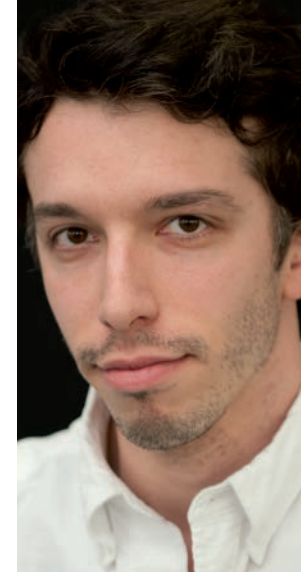
Pedro López-García

Researcher

Pedro López-García received a MS degree and a Ph.D. in Computer Science from the Technical University of Madrid (UPM), Spain in 1994 and 2000, respectively. In May 28, 2008 he obtained a Scientific Researcher position at the Spanish Council for Scientific Research (CSIC) and joined the IMDEA Software Institute. Immediately prior to this position, he held associate and assistant professor positions at UPM and was deputy director of the Artificial Intelligence unit at the Computer Science Department. He has published about 54 refereed scientific papers, many of them at conferences and journals of high or very high impact. He served as the scientific local coordinator of the European project ES_PASS "Embedded Software Product-based ASSurance," and is currently the principal investigator at the institute of the European FP7 FET project ENTRA "Whole-Systems Energy Transparency." He has also participated as a researcher in many other regional, national, and international projects.

Research Interests

His main areas of interest include energy-aware software engineering; automatic analysis and verification of non-functional program properties such as resource usage (energy, execution time, user defined, etc.), non-failure and determinism; performance debugging; abstract interpretation; (automatic) granularity analysis/control for parallel and distributed computing; combined static/dynamic verification and unit-testing; tree automata; constraint and logic programming.



Michael Emmi

Researcher

Michael received his Ph.D. in Computer Science from UCLA in 2010 and joined the IMDEA Software Institute in 2013, following a postdoc fellowship at the Université Paris Diderot awarded by La Fondation Sciences Mathématiques de Paris. Prior to all that, Michael completed his undergraduate studies at Binghamton University (SUNY). He has been a teaching assistant for undergraduate courses at UCLA and Université Paris Diderot, and has held internships at Microsoft Research, NASA Ames Research Center, and IBM.

Research Interests

Michael's research enables the construction of reliable software by developing the foundations for effective programming abstractions and informative program analysis tools. Integrating technological trends with knowledge from several research communities spanning automata theory, programming languages, and distributed systems, his contributions include establishing the theoretical limits of program analysis, devising tractable approximations for intractable analysis problems, and building effective analysis tools.

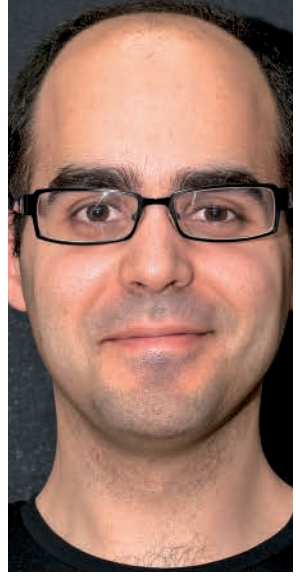
Pierre-Yves Strub

Researcher

Pierre-Yves Strub received his Ph.D. in Computer Science from École Polytechnique, France, in 2008. He joined the IMDEA Software Institute in 2013, after a postdoctoral position at the Microsoft-INRIA Joint Lab in Paris, France and at the LIAMA institute in Beijing, China.

Research Interests

Pierre-Yves research interests include formal proofs, proof assistants and their related type theory, certification of cryptographic algorithms and mathematical proofs, program verification via typing, and secure web programming. He is currently focused on EasyCrypt, a toolset for reasoning about relational properties of probabilistic computations with adversarial code, of which he is one of the main authors. He is also the main author of CoqMT, an extension of the Coq proof assistant.



José Francisco Morales

Researcher

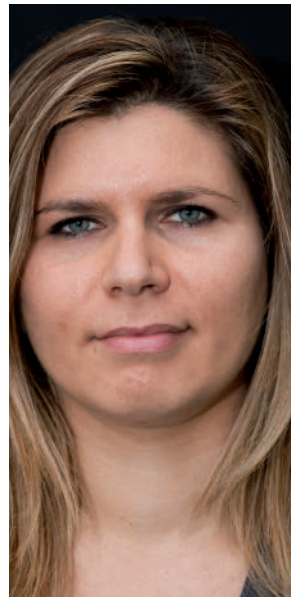
Jose F. Morales joined the IMDEA Software Institute as a postdoctoral researcher in November 2011, after receiving his Ph.D degree in Computer Science from the Technical University of Madrid (UPM), Spain. Previously, he held a teaching assistant position at the Universidad Complutense de Madrid, starting in 2005.

Jose's work to date has focused on mechanisms for the efficient execution of logic programs: inference of program properties by abstract interpretation, highly-optimizing translation to low-level code using those properties, and the development of abstractions for the specification and automated construction of abstract machines.

Research Interests

His current research interests include the design of multiparadigm languages (combining imperative, logic, functional, and object-oriented programming), assertion languages and type systems, abstract interpretation, abstract machines, compiler optimizations, and native code generation.

postdoctoral researchers



Zorana Banković

Postdoctoral researcher

Zorana Banković obtained her Electrical Engineer degree from the Faculty of Electrical Engineering at the University of Belgrade (Serbia) in 2005 and her Ph.D. degree from the Universidad Politécnica de Madrid (UPM) in 2011. Her dissertation was given the UPM special award as one of the four best theses of Telecommunications School that year. Before joining IMDEA Software, she was a researcher at the Department of Electronic Engineering at UPM. She has participated in 11 research and development projects, and authored 10 journal publications. During that time her main research interests included energy-efficient security solutions for wireless sensor networks, anomaly detection and thermal–aware optimizations in data centers, such as floor planning, dynamic resource scheduling and allocation, as well as the design of a reputation system, that allows applying optimization techniques to each state of a data center.

After joining IMDEA Software in October 2012, her research has mainly been related to ENTRA research project, funded by the EU 7th Framework Program Future and Emerging Technologies (FET).

Research Interests

Her current research interests are in "energy-aware" software development using advanced program analysis and modeling of energy consumption in computer systems, aimed at making predictions of energy consumption early in the software design phase, and therefore enabling the development of greener IT through energy-efficient usage of hardware resources. Zorana's work includes research and development of energy optimization techniques at all software levels (compiler, OS, algorithms), as well as identification of static analyses that provide necessary input to the optimization stages which aim at improving resource consumption.

François Dupressoir

Postdoctoral researcher

François Dupressoir joined the IMDEA Software Institute as a postdoctoral researcher in February 2013. He successfully defended his Ph.D. in Computer Science at the Open University (U.K.) under the supervision of Andy Gordon, Jan Jürjens, and Bashar Nuseibeh. His Ph.D. studies were partially funded by a Microsoft Research Ph.D. scholarship, and led him to internships at the European Microsoft Innovation Center, and at Microsoft Research in Redmond and Cambridge. During those stays, he participated in the development of the VCC general-purpose verifier for C, and applied it to proving cryptographic security properties of the TPM's reference implementation.

Research Interests

François is broadly interested in program verification, theorem proving and cryptography. He is currently working on methods for formally reasoning about cryptographic security properties of real-world systems, especially focusing on obtaining strong correctness and security results on low-level implementations of schemes and protocols in presence of strong adversaries that may break abstractions, for example by observing side-channels or injecting faults in the execution of the cryptographic systems. Of particular interest is the study of how compilation can be made 'security aware', by ensuring that strong security properties are preserved by compilation, and by developing compilation techniques that prevent lower-level adversaries from exploiting their abstraction-breaking capabilities to break the security of the system.

Benedikt Schmidt

Postdoctoral researcher

Benedikt Schmidt joined the IMDEA Software Institute as a postdoctoral researcher in February 2013. He received his Ph.D. degree in Computer Science from ETH Zurich, under the supervision of David Basin.

Research Interests

Benedikt is broadly interested in the areas of theorem proving, program verification, and rewriting and in their application to analyzing cryptographic systems. During his PhD, his work has focused on the symbolic analysis of security protocols including interactive machine-checked approaches and fully automated approaches. Since then, he has extended his focus to the computational model of attacks and is working on methods that combine the advantages of symbolic and computational models. Namely, these methods are mostly (or even fully) automated, can deal with cryptographic assumptions, cryptographic primitives, and cryptographic protocols, and provide guarantees with respect to the standard computational attacker models used in cryptography.

Ilya Sergey

Postdoctoral researcher

Ilya Sergey joined the IMDEA Software Institute as a postdoctoral researcher in December 2012. He received his Ph.D. degree in Computer Science from KU Leuven (Belgium) under the supervision of Dave Clarke in November 2012. During his doctoral studies he was a visiting Ph.D. fellow at the Department of Computer Science of Aarhus University (Denmark), hosted by Olivier Danvy, and a research intern in the Programming Principles and Tools group at Microsoft Research Cambridge (UK), supervised by Simon Peyton Jones.

Research Interests

Ilya's research interests dwell in the area of the programming languages design and implementation. He has published papers at PLDI, POPL, ESOP, ICFP, and many other venues. Ilya is mostly interested in the design of scalable, robust, and intellectually manageable methodologies for program analysis and verification. His mission is to increase understanding of principles of software construction with a concrete goal in mind: development of improved tools for computer-aided programming and verification. As a researcher at IMDEA, Ilya is working with Aleks Nanevski and Anindya Banerjee on verification techniques, developing a type-theoretic approach to specification and checking of properties of higher-order concurrent programs.

Dragan Ivanović

Postdoctoral researcher

Before joining IMDEA Software, Dragan Ivanović received his B.Sc. and M.Sc. degrees in Computer Science and Electrical Engineering from University of Sarajevo, Bosnia and Hercegovina, and PhD in Computer Science from the Technical University of Madrid (UPM). His doctoral studies mainly concentrated on employing logic and constraint modeling and programming, as well as the corresponding program analysis methods, to study properties of complex and adaptive service oriented computing systems. He received the best paper award at ICSOC 2011.

Research Interests

His main research interests are currently related to using computational logic and constraint programming techniques to model and analyze properties of complex adaptive software systems, such as service compositions provided via cloud. His other interests include dynamic modeling of cloud provision systems, and study of probabilistic behavior of service compositions, in terms of their performance and other non-functional properties.

Andrea Cerone

Postdoctoral researcher

Andrea Cerone obtained his Ph.D. in November 2012, from Trinity College Dublin. During his Ph.D. his work focused on applications of process algebras and behavioral theories to distributed systems, with a particular emphasis to wireless networks and probabilistic distributed systems. He joined the IMDEA Software Institute as a postdoctoral researcher in June 2013, his research focuses switched to the development of proof methods for verifying higher order, concurrent software, where he also started developing formal verification techniques for higher order, concurrent programs, as well as investigating the mathematical foundations of modern distributed database systems.

Research Interests

Andrea's main line of research concerns the understanding of the mathematical theory underlying modern geo-replicated and distributed databases, as well as the applications of such a theory to practical applications; these include the formal verification of concurrency control mechanisms, as well as the development of techniques for boosting the performances of geo-replicated databases. He is also interested in the understanding of behavioral theories in different concurrent models of computation. These range over a wide spectrum, including linearisability for multithreaded programs, testing preorders for distributed systems with both non-deterministic and probabilistic behavior.

Guillermo Vigueras

Postdoctoral researcher

Guillermo Vigueras joined IMDEA Software Institute as a postdoctoral researcher in November 2013. He received his PhD degree in Computer Science from University of Valencia (Spain). During his PhD he did several internships at different European institutions and research groups like the Distributed Systems and Middleware Group at INRIA-Rennes, under the supervision of Thierry Priol. Before joining IMDEA he worked as a postdoctoral researcher at the Biomedical Engineering Department of King's College London (KCL) and IMDEA Materials Institute where he worked within multidisciplinary teams for computer simulation of different scientific and engineering problems. During his stay at KCL he developed the first GPU implementation of human cardiac electro-mechanical models for assisting in patient specific diagnosis.

Research Interests

In the past his research interests were related with different areas like: meta-heuristic optimization and code parallelization for the exploitation of heterogeneous computer architectures like HPC and embedded platforms. Now at IMDEA Software Institute he is applying his previous experience to work on automatic transformation of programs for tackling the complexity of efficiently programming heterogeneous platforms.

Rémy Haemmerlé

Postdoctoral researcher

Rémy prepared is Ph.D. in Computer Science at INRIA Rocquencourt, France and received his degree from the Université Paris Diderot in January 2008. He joined the IMDEA Software institute in 2014, after a post-doctoral position at the Technical Univer.

Research Interests

Rémy is primarily interested in studying the formal properties of logical programming languages with constraints, and more specifically CHR (Constraint Handling Rules) a high-level rules-based language. In particular he recently improved several results about confluence and logical completeness of this language. He is also interested in compilation and static analysis, as it applies to logical languages.

Giovanni Bernardi

Postdoctoral researcher

Giovanni obtained his BSc and MSc in computer science from Ca'Foscari, the University of Venice, and during his Erasmus year studied bioinformatics at the University of Leiden. Giovanni obtained the PhD in November 2013, from Trinity College Dublin, and after two PostDocs, one in Dublin, and a short one at the Universidade de Lisboa, he arrived at IMDEA Software.

Research Interests

Giovanni's main research interest is semantics of programming languages, so he often plays with type theory, unification, static analysis, concurrency theory, weak consistency, and distributed systems. Giovanni's PhD thesis unravels a series of behavioral equivalences for clients and peers within two settings, the Calculus of Communicating Systems, and higher-order session types. Subsequent work by Giovanni provides a (fully-abstract) semantic explanation of the standard subtyping for session types, and questions the existing notions of duality for these types. At present Giovanni is working towards the foundations of weak consistency levels for distributed databases.

visiting faculty

Michael Ernst

Visiting Professor

University of Washington, USA

Visiting during
Sep. 2014 – Jan. 2015

Roberto Giacobazzi

Visiting Professor

University of Verona, Italy

Visiting during
Oct. 2014 – Sep. 2015.

research assistants

Research Assistants hold full scholarships or contracts at the Institute, performing research within one of the Institute's research lines under the supervision of a junior or senior researcher, and they undertake their Ph.D. at one of the Universities that the Institute has agreements with. Many of our Research Assistants obtain their degrees from the Technical University of Madrid (UPM), with whom the Institute collaborates in the development of graduate programs, and also at Universidad Complutense de Madrid (UCM).

Álvaro García

Research Assistant

Degree: Technical University of Madrid (UPM), Spain

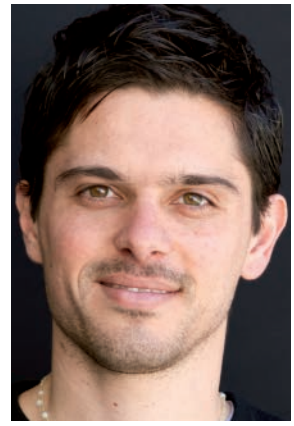
Research: Efficient implementations of functional programming languages: theories and models for higher-order languages and lambda calculus, inter-derivation of program semantics, and abstract machines.

Miguel Angel García de Dios

Research Assistant

Degree: Universidad Complutense de Madrid (UCM), Spain

Research: Formal specification and verification, software engineering, and security; rigorous tool supported modeling and validation of software systems.

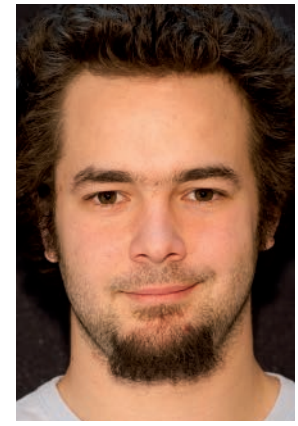


Julian Samborski-Forlese

Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Applications of formal methods and abstract interpretation to program verification; quantum computing; functional programming languages; semantics.



Juan Manuel Crespo

Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Relational logics; formal verification of cryptographic primitives and protocols; programming languages.

Federico Olmedo
Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Verification of cryptographic systems and semantics of programming languages.

Alejandro Sánchez
Research Assistant

Degree: Universidad Nacional de Córdoba (UNC), Argentina

Research: Formal verification of temporal properties in concurrent systems, development of deductive techniques for the verification of parameterized systems and construction of specialized decision procedures for complex data structures that manipulate dynamic memory.

Carolina Inés Dania
Research Assistant

Degree: Universidad Nacional de Córdoba (UNC), Argentina

Research: Software engineering, formal methods and security. In particular, working on tools and techniques for modeling, building and validating secure and reliable software systems.

Germán Andrés Delbianco
Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Germán's research has focused lately on the design and implementation of new dependently-typed theories aimed at reasoning about, and proving the correctness of, higher-order programs with unstructured stateful features e.g., continuations, fork/join concurrency and coroutines, from a computational effects perspective.

Umer Liqat
Research Assistant

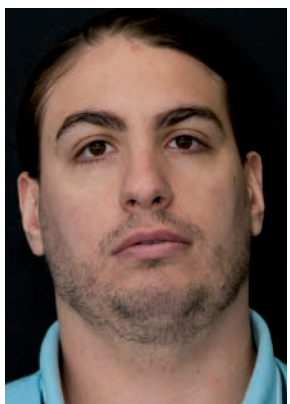
Degree: Technical University of Madrid (UPM) and Dresden University of Technology (TUD), Germany

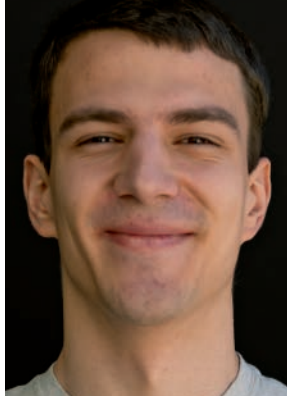
Research: Static resource analysis and verification of non-functional program properties (execution time, energy, etc.) and its applications to Energy-aware software engineering, transformation-based analysis framework for multi-language analysis and optimizations trading-off precision/performance/energy.

Antonio Nappa
Research Assistant

Degree: Università degli Studi di Milano, Italy

Research: Computer security; malware analysis and cybercrime.





Artem Khyzha
Research Assistant

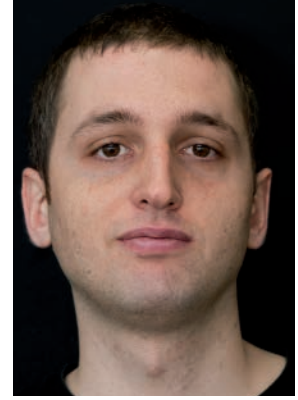
Degree: Technical University of Madrid (UPM), Spain

Research: Developing a generalized compositional reasoning technique for proving linearisability of fine-grained concurrent programs operating on a shared memory such as non-blocking algorithms.

Miriam García
Research Assistant

Degree: MSc in Mathematical Modeling in Engineering, University of L'Aquila and University of Hamburg

Research: Stability analysis based on model-checking techniques; hybrid systems; applied mathematics (PDEs, dynamical systems).



Goran Doychev
Research Assistant

Degree: M.Sc. from Saarland University, Germany

Research: Obtaining quantitative security guarantees for computer systems, and using them to develop economically justified defenses. Favorite application: Side-channel attacks.

Nataliia Stulova
Research Assistant

Degree: MSc in Artificial Intelligence, Technical University of Madrid (UPM), Spain

Research: Assertion languages, their design and use for program specification, program instrumentation and automatic source code documentation. Assertion-based run-time software verification and debugging. Combination of static and dynamic program analyses. Applications to (Constraint) Logic Programming.

Maximiliano Klemen
Research Assistant

Degree: BS, Universidad Nacional del Comahue (UNCo), Argentina

Research: Abstract interpretation-based static analysis for inferring energy consumption information about (concurrent) program executions. He is working on the FP7 project "Whole-Systems ENergy TRAnsparency" (ENTRA).

Joaquín Arias
Research Assistant

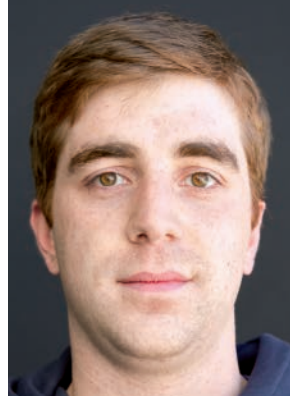
Degree: Technical University of Madrid (UPM), Spain

Research: Design and implementation of advanced programming languages, including logic programming languages featuring constraints and tabling.

Ratan Lal
Research Assistant

Degree: Indian Statistical institute, Kolkata, India

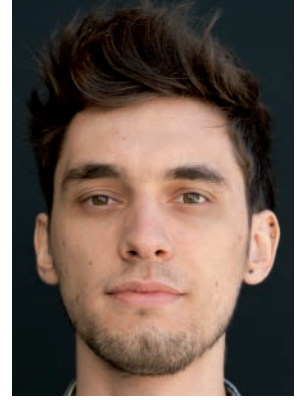
Research: Reachability analysis of linear dynamical system with uncertain parameter, non linear dynamical system, application of reachability analysis in compositional verification.



Luca Nizzardo
Research Assistant

Degree: Università degli Studi di Milano-Bicocca, Italy

Research: Cryptography and its applications to cloud computing security, homomorphic signatures.



Damir Valput
Research Assistant

Degree: University of Zagreb, Croatia

Research: Applications of automata theory to solving problems in formal languages, signal processing, transducers, and verification.

Miguel Ambrona
Research Assistant

Degree: Universidad Complutense de Madrid (UCM), Spain

Research: Computer-aided cryptographic proofs with particular emphasis on Structure Preserving Signature schemes.

Irfan Ul Haq
Research Assistant

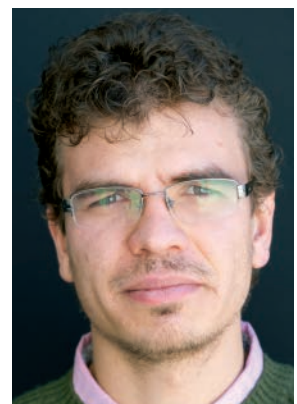
Degree: National University of Sciences and Technology (NUST), Islamabad, Pakistan

Research: Use of Natural Language Processing (NLP) techniques to realize potential bugs in software. Binary/malware analysis and application layer security.

Raúl Alborodo
Research Assistant

Degree: BS in computer Science, Universidad Nacional de Río Cuarto (UNRC), Argentina

Research: Model-based construction of reliable concurrent software, software specification and verification, model-driven development for concurrency.



interns

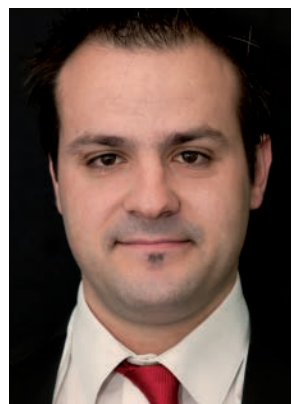
Intern	Period	Nationality
Alejandro Ranchal	Sep. 2014 – Jul. 2015	Spain
Burcu Ozkan	Apr. – Jul. 2014	Turkey
Elena Gutierrez	Jun. – Aug. 2014	Spain
Guillermo Ramos	Jul. 2013 – Jun. 2015	Spain
Javier del Valle	Jun. – Sep. 2014	Spain
Justin Hsu	May – Sep. 2014	United States
Lavinia Damian	Oct. 2013 – Apr. 2014	Romania
Marcos Sebastián	Oct. 2014 – Dec. 2015	Spain
Pedro Valero	Jun. 2014 – Apr. 2015	Spain
Platon Kotzias	May. 2014 – Jan. 2015	Greece
Rana Faisal Munir	Nov. 2014 – Nov. 2015	Pakistan
Santiago Cervantes	Sep. 2014 – Mar. 2015	Spain
Simón Cancela	Oct. 2014 – Apr. 2015	Spain

project staff
joint research units

Project Staff provide additional support for the development of projects and contracts being carried out at the Institute. They are typically co-funded by such projects.

Guillermo Jiménez
Technical Project Staff,
Telefónica Joint Research Unit

Degree: B.Sc., European University Miguel de Cervantes, Valladolid, Spain



Beatriz Muñoz
Technical Project Staff,
Telefónica Joint Research Unit

Degree: B.Sc., University Rey Juan Carlos, Madrid, Spain

Leandro Guillén
Technical Project Staff,
Telefónica Joint Research Unit

Degree: MS in Professional Development, Universidad de Alcalá de Henares, Spain

project management and technology transfer unit

Jesús Contreras
Project Strategy Manager
& Business Developer

Degree: MBA - CEREM and PhD in CS - Technical University of Madrid (UPM), Spain

Juan José Collazo
Project Manager

Degree: B.Sc. in Economic Sciences-Complutense University, Madrid, Spain

David García
Social Media & Web Manager

Degree: MA Visual Anthropology, Goldsmiths College, University of London, UK

technical support and infrastructures unit

Research Support Technical Staff provide support for the research infrastructures provided to the researchers at the Institute. These include virtualization environments, version control systems, research collaboration tools, continuous integration platforms, experimentation harnesses, computing farms, communications, etc. They are currently co-funded by different projects and agreements.

Roberto Lumbreras
Computing and Communication Infrastructures

Degree: MSc. Elec. & Computer Eng. Technical University of Madrid (UPM), Spain

Juan Céspedes
Network and Systems Engineer

Degree: MSc. Elec. & Computer Eng. Technical University of Madrid (UPM), Spain

Gabriel Trujillo
Systems Administrator

Degree: AD in Network Systems Administration, El Rincón, Las Palmas, Spain

management
& administration

María Alcaraz
General Manager

Degree: MBA - Escuela Internacional de Negocios – CEREM, Madrid, Spain

Paola Huerta
Human Resources Assistant
(part-time)

Degree: M.A. in Art History – Universidad Complutense, Madrid, Spain

Tania Rodríguez
Administrative Assistant
(part-time)

Degree: M.Sc. in Business Administration – Universidad Centroamericana José Simeón Cañas

Laura Bellmont
Infrastructure Manager

Degree: M.Sc. in Architecture – Technical University of Madrid (UPM), Spain.

Begoña Moreno
IMDEA Common Services
(part-time)

Degree: Ph.D. in Economics and Political Sciences

Andrea Iannetta
Administrative Assistant

Degree: B.Sc. in Economics – Godspell College, Argentina

Carlota Gil
Accounting Assistant
(part-time)

Degree: M.Sc. in Business Administration – Universidad Rey Juan Carlos, Madrid, Spain

research projects and contracts

5.1. Projects Running in 2014 **[62]**

5.2. Fellowships **[74]**

annual report 2014

An important source of funding and technology transfer opportunities for the Institute are cooperative projects, awarded through competitive calls for proposals by national and international funding agencies, and contracts with industry. During 2014, the Institute participated in a total of 29 funded research projects and contracts, the majority of which (23, 79%) involve collaboration with industry. Of the 29 projects, 15 are from international agencies (14 funded by the European Union and 1 by the US ONR and Stanford University), 8 of them are direct industrial funding, and the rest are funded by national (4) and regional (2) agencies. Figure 5.1 shows the origin of project funding. In the same year, the Institute benefited from 15 fellowships.

The trend of external funding for the period 2008-2014 is shown in Figure 5.2, together with the forecast figures for 2014 and for 2015. The amount of external funding (and the percentage of external to total funding) has risen from around 1.1 M€(30%) in 2013 to 1.96 M€(42%) in 2014, which is well beyond the projections for 2014 performed at the end of 2013 (1.3 M€). This is due in part to new projects, and also to the finalization of a number of projects in 2014 and to the temporary need to handle certain EIT ICT Labs partner activities by the Institute. The level of external funding is expected to stabilize around 1.75 M€ (40%) in 2015 (still within the growing trend with respect to 2013), once these temporary factors disappear.

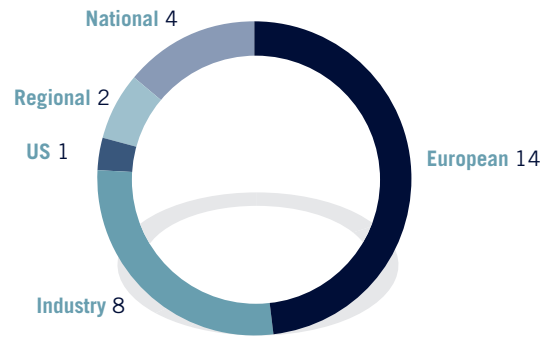


Figure 5.1: Projects by origin of funding.

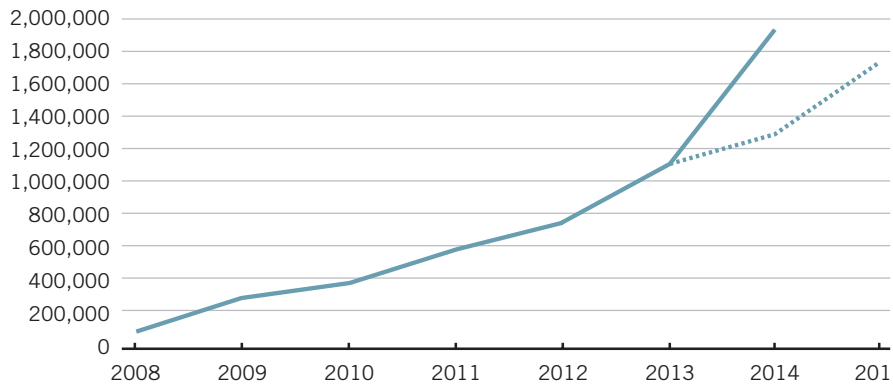


Figure 5.2: Evolution in external funding since 2008.

5.1. Projects Running in 2014

CADENCE

Cyber Attack Detector Engineering for Commercial Exploitation

Funding: European Institute of Innovation and Technology
Duration: 2014
Principal Investigator: Asst. Res. Prof. Juan Caballero

The CADENCE project is a year-long action and a part of the EIT ICT Labs activities in 2014 in its Action Line on Privacy, Security, and Trust. The project concentrates on development of a sensor able to detect advanced cyber attacks in network traffic by applying innovative anomaly detection technology, with the goal of advancing cyber-defense expertise and creating more secure ICT environments in both governments and businesses. CADENCE aims at addressing the needs of a segment of a market whose size is estimated at 250 billion EUR in Europe with specific innovative product and service prototypes. The project was developed together with TNO in Netherlands, and the Reply Spa. group in Italy.

I3H

Incubating Internet Innovation Hubs

Funding: European Union – 7th Framework Program
Duration: 2014–2016
Principal investigator: Res. Prof. Juan José Moreno

The objective of the I3H project is to contribute to the sustainability of the FI PPP by creating a European network of Internet Innovation Hubs (IIH), regional or thematic clusters that bring together web entrepreneurs, mentors, investors, students, academia, industry, and public sector innovators to speed up the transformation of FI PPP results to services and applications addressing the needs of European citizens, companies, and society. The starting point is the initial network of EIT ICT Labs hubs in Budapest, Eindhoven, Helsinki, Madrid, Paris and Trento coinciding with the Nodes of EIT ICT Labs. The seed network will grow organically with a robust life-cycle incubation stage gate process for identifying candidate hubs and guiding them through tangible milestones towards full-fledged IIH's with hands-on coaching, resources and support, including knowledge and best practice transfer.

Comunidad de Madrid
La Suma de Todos

N-GREENS

Next-Generation Energy-Efficient Secure Software

Funding: Regional Government of Madrid
Duration: 2014–2017
Project Coordinator: Res. Prof. Gilles Barthe

The N-GREENS software addresses the ever growing economic and strategic significance of the software industry, the presence and ubiquity of software and computer devices in everyday life, and the resulting need for revolutionary solutions to enable citizens to access myriads of such services in a secure and sustainable way. Along with a strong research component carried out by a world-class expert consortium, the project has a strong technology transfer component. The N-GREENS Project aims at developing disruptive technologies in some of the key areas with a high social impact. Its technical areas include: green computation, cloud security, cyber-physical systems, parallelism for the masses, and the resulting software tools.

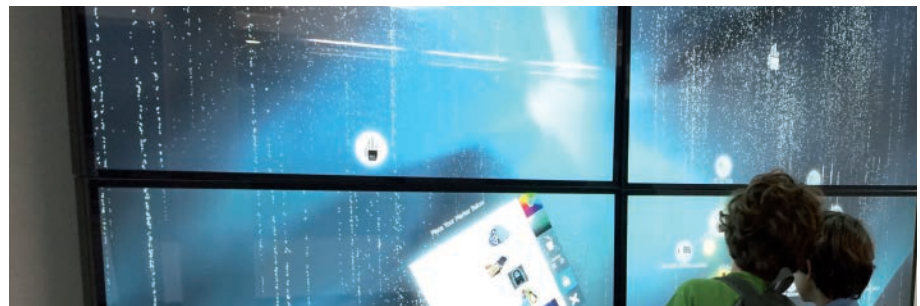
N-GREENS is a consortium involving groups from Universidad Complutense de Madrid, Universidad Politécnica de Madrid, and the IMDEA Software Institute, which is the project coordinator.

VerisTab

Formal Verification of Stability of Embedded Control Systems Funding: European Union – 7th Framework Program

Duration: 2013–2016
Principal investigator: Asst. Res. Prof. Pavithra Prabhakar

The VerisTab project addresses the challenge of building high confidence embedded control systems, by means of verifying their stability (resistance to perturbation in the initial state or inputs) using automated formal verification techniques that will be developed within the project. The objective is to facilitate the development of fully automated and scalable methods for stability verification, thereby addressing the shortcomings of the state-of-the-art deductive techniques. An algorithmic approach to stability verification is a challenging task, since, even fundamental notions for abstraction and composition, which form the backbone of scalable algorithmic verification, have not been well explored. VerisTab proposes a three-phase plan from developing theoretical foundations to algorithm design and software tool development.



ADVENT

Architecture-Driven Verification of Systems Software

Funding: European Union – 7th Framework Program – FET Young Explorers
Duration: 2013–2016
Project Coordinator: Asst. Res. Prof. Alexey Gotsman

IMDEA Software is the main partner and coordinator of the ADVENT research project. The project was awarded during the year 2012 and runs from April 2013 to 2016. It is funded by the very competitive EU 7th Framework Program, Future and Emerging Technologies (FET) *Young Explorers Initiative*, and has an overall budget of 1 million Euro. In addition to IMDEA Software, the consortium includes as partners Tel Aviv University (Israel), The Max Planck Institute (Germany), and Katholieke Universiteit Leuven (Belgium).

The ADVENT project (http://advent-project.eu) develops innovative methods and tools for cost-effective verification of real-world systems software, making it possible to guarantee an unprecedented level of reliability. ADVENT will achieve this by exploiting a trend among programmers to use informally described patterns, idioms, abstractions, and other forms of structure contained in their software, which are together called its architecture.

Building on the emerging technology of separation logic, ADVENT will formalize such software engineering concepts used by systems programmers to reason about their software informally, and will use the results to drive the design of verification techniques. This is a radically novel approach to the problem of verifying complex software: it departs from the common practice of building generic verification tools that, not being able to take advantage of programmers' knowledge and intuition, do not scale to big and complicated systems.

The architecture-driven verification techniques resulting from the project have the potential to yield a dramatic leap in the cost-benefit ratio of verification technology. This will allow verification to scale to systems of real-world size and complexity that so far have been beyond the reach of quality assurance methods guaranteeing correctness.

POLCA

Programming Large Scale Heterogeneous Infrastructures

Funding: European Union – 7th Framework Program
Duration: 2013–2016
Principal Investigator: Assoc. Res. Prof. Manuel Carro

The POLCA project explicitly addresses the programmability concerns of both embedded and high performance computing. Both domains have generated strongly focused approaches for solving their specific problems that are now confronted with the increasing need for parallelism even in Embedded Systems and the need for addressing non-functional criteria in High Performance Computing. Rather than improving both domains separately, POLCA takes a bold step forward by proposing a hybrid programming model that decisively increases programming efficiency in both areas and enables realization of multi-domain use cases.

This model thereby allows efficient parallelization and distribution of the application code across a highly heterogeneous infrastructure, not through automatic methods, but through exploitation of fundamental mathematical axioms behind the execution logic. The model is strongly oriented towards mathematical application cases of both domains, ranging from sensor evaluation, over monitoring-control-loops to complex simulation and modeling. POLCA is thereby explicitly geared towards exploitation of reconfigurable hardware to make use of their high efficiency under the right usage criteria. In principal it even allows for exploitation of run-time reconfigurations, given an application with a suitable profile.

The project builds up on existing collaboration between experts from embedded computing and high performance computing, to combine complementary expertise from the two domains into an accessible and productive programming model of the future.

ENTRA

Whole-systems energy transparency

Funding: European Union - 7th Framework Program - FET proactive MINECC call
Duration: 2012-2015
Project Coordinator: Res. Prof. John Gallagher

ENTRA is an FP7 “Future and Emerging Technologies” project under the proactive “MINECC” objective - “Minimizing Energy Consumption of Computing to the Limit”. The ENTRA project proposes radical advances in energy-aware software design and management with the objective of providing an important key to the pervasive realization

of energy-aware computing. Though huge advances have been made in power-efficient hardware, most of the potential energy savings are wasted by software that does not exploit energy-saving features of hardware, and by poor dynamic management of tasks and resources. The budget of the project is approximately 2.7M Euros.

The project is built around the central concept of *energy transparency* at every stage of the software lifecycle. The project develops novel *program analysis* and *energy modeling* techniques, making energy usage transparent through the system layers. This will enable *energy optimizations* both during code development and at run-time, and promote energy efficiency to a first-class software design objective.

AutoCrypt

Funding: US Office of Naval Research (ONR), through Stanford University
Duration: 2012-2015
Project Coordinator: Res. Prof. Gilles Barthe

AutoCrypt is a joint project with Stanford University, University of Pennsylvania, and SRI, funded by ONR and which runs from July 2012 until July 2015. It has an overall budget of 2 Million Euros. AutoCrypt aims to use computer technology to provide mathematical guarantees that a cryptographic algorithm is secure, and that it is adequate for a given product, process, or service.

Within the project, the IMDEA Software team use their EasyCrypt tool (http://www.easycrypt.info) to develop a systematic classification of cryptographic algorithms and to create a cryptographic atlas that will be used by researchers and companies to choose the most suitable algorithm for their needs.

NESSoS

Network of Excellence on Engineering Secure Future Internet Software Services and Systems

Funding: European Union, Cooperation Program (NoE) – 7th Framework Program
Duration: 2011-2014
Principal Investigator: Assoc. Res. Prof. Manuel Clavel

The Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS) aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. The NESSoS consortium

involves 12 partners, including 2 companies (namely, Siemens and ATOS), from 7 countries. The budget for the project is approximately 3.5 M Euros.

The domain of Engineering Secure Software Services covers a collection of engineering activities that aim at the creation of software services —i.e. ICT services delivered through the deployment of software systems— that are both behaviorally correct (typically guided by software engineering principles) as well as secure (typically guided by security engineering principles). The approach of engineering secure software services is based on the principle of addressing security issues from the very beginning in system design and analysis, thus contributing to reducing system and service vulnerabilities, improving the necessary assurance level, thereby considering risk and cost issues during development in order to prioritize investments.

IMDEA Software plays a prominent role in three research workpackages: secure service architectures and design; programming environments for secure and composable services; and security assurance for services. Also, IMDEA Software leads the researcher mobility program within the consortium. This program is a mechanism that supports the integration of activities across the various sites: it brings together researchers working on related topics; it drives knowledge exchange and knowledge generation through union and diversity; and, finally, it increases the capability of joint cooperation among researchers.

VARIES

ARTEMIS

Hi iberia

INTEGRASYS

tecnalia Inspiring Business

VARIES

Variability in safety critical embedded systems

Funding: ARTEMIS- European Union - 7th Framework Program
Duration: 2012-2015
Principal Investigator: Asst. Res. Prof. Aleksandar Nanevski

VARIES is an ARTEMIS Joint Undertaking project granted under the FP7 ARTEMIS-2011-1 Call. The 26 partner-strong international consortium includes the participation of national partners Hi-Iberia, Integrasys, and Tecnalia. The main goal of the VARIES project is to help Embedded Systems (ES) developers to maximize the full potential of variability in safety-critical ES. The objectives of this project will be therefore (i) to enable companies to make informed decisions on variability use in safety-critical ES; (ii) to provide effective variability architectures and approaches for safety-critical ES; and (iii) to offer consistent, integrated, and continuous variability management over the entire product life cycle.

The VARIES project develops the VARIES Platform: a complete, cross-domain, multi-concern, state-of-the-art reference platform for managing variability in safety-critical

ES. Special attention is given to aspects specific to safety-critical ES, in particular the impact of reuse and composition on certification.

In addition to this ambitious goal, the VARIES project will create a Center of Innovation Excellence (CoIE) for managing variability in ES. The VARIES CoIE will support the European ES industry on the 3 aforementioned objectives.

DESAFIOS-10

High-Quality, Reliable, Distributed, and Secure Software Development

Funding: Spanish Ministry of Science and Innovation
Duration: 2011-2014
Principal Investigator: Res. Prof. Gilles Barthe

The overall goal of the DESAFIOS-10 project is to contribute both foundations and technologies for the development of software systems with certified quality and reliability, based on formal methods and declarative programming. The consortium involves groups from three different Institutions (Universidad Complutense de Madrid, Universidad Politécnica de Madrid, and IMDEA Software) and a number of industrial users.

This project arises as a natural evolution of the previous coordinated project DESAFIOS, which involved only the research groups from Universidad Complutense de Madrid and Universidad Politécnica de Madrid. In contrast, DESAFIOS-10 emphasizes the security and reliability aspects of this research, which is precisely the workpackage led by IMDEA Software.

PROMETIDOS

Methods for Rigorous Software Development

Funding: Regional Government of Madrid
Duration: 2011-2014
Principal Investigator: Res. Prof. Gilles Barthe

The PROMETIDOS-CM research program is focused on four main areas: specification and validation, to provide a solid foundation for the description and analysis of services; reliability and security, to guarantee robust solutions from start to end; declarative programming, to develop the next generation of languages for services; and efficiency, to optimize quality of service with respect to performance. A common goal for all these research lines is the development of tools that will rigorously support their scientific results and that can be eventually transferred to industry.

PROMETIDOS-CM is a consortium involving groups from Universidad Complutense de Madrid, Universidad Politécnica de Madrid, and the IMDEA Software Institute, which is the project coordinator.

StrongSoft

Sound Technologies for Reliable, Open, New Generation Software

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2013–2015
Principal Investigator: Res. Prof. Gilles Barthe

The goal of the StrongSoft project is to define, implement, evaluate, and disseminate disruptive technologies that are able to keep pace with the rapid evolution of software systems and address the challenges it implies. The project provides solutions for supporting the cost-effective development of a new generation of software systems that are reliable, efficient, and secure while connected to an open, untrusted world, across different application domains. The workplan is organized in a number of coordinated lines that cover security and cryptography, verification, debugging and testing, language technology, and tools. To achieve its objectives the StrongSoft consortium coordinates some of Spain's leading research groups in reliable software technologies together with a number of key foreign researchers and highly interested industrial end users.

ARVI

Runtime Verification Beyond Monitoring

Funding: European Union, COST Action
Duration: 2014–2018
Investigator: Res. Prof. César Sánchez

Runtime verification (RV) is a computing analysis paradigm based on observing a system at runtime to check its expected behavior. RV has emerged in recent years as a practical application of formal verification, and a less ad-hoc approach to conventional testing by building monitors from formal specifications. There is a great potential applicability of RV beyond software reliability, if one allows monitors to interact back with the observed system, and generalizes to new domains beyond computer programs (like hardware, devices, cloud computing, and even human-centric systems). Given the European leadership in computer

based industries, novel applications of RV to these areas can have an enormous impact in terms of the new class of designs enabled and their reliability and cost effectiveness.

CryptoAction

Cryptography for Secure Digital Interaction

Funding: European Union, COST Action
Duration: 2014–2018
Investigator: Ass. Res. Prof. Dario Fiore

As increasing amounts of sensitive data are exchanged and processed every day on the Internet, the need for security is paramount. Cryptography is the fundamental tool for securing digital interactions, and allows much more than secure communication: recent breakthroughs in cryptography enable the protection – at least from a theoretical point of view – of any interactive data processing task. This includes electronic voting, outsourcing of storage and computation, e-payments, electronic auctions, etc. However, as cryptography advances and becomes more complex, single research groups become specialized and lose contact with "the big picture". Fragmentation in this field can be dangerous, as a chain is only as strong as its weakest link. To ensure that the ideas produced in Europe's many excellent research groups will have a practical impact, coordination among national efforts and different skills is needed. The aim of this COST Action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments. The Action will foster a network of European research centers thus promoting movement of ideas and people between partners.

AMAROUT II Europe

Funding: European Union, Marie Curie Action (PEOPLE-COFUND) - 7th Framework Program
Duration: 2012-2016
General Coordinator: Res. Prof. Manuel Hermenegildo

AMAROUT-II Europe is a PEOPLE-COFUND Marie Curie Action which continues the AMAROUT action sharing with it the objectives of fostering and consolidating the European Research Area by attracting top research talent to Europe and, in particular, to the region of Madrid. As in the previous AMAROUT program, "experienced" and "very experienced" researchers from any country can apply for AMAROUT II fellowships at any of the seven IMDEA Institutes participating in the program (Energy, Food, Materials, Nanoscience, Networks, Software, and Water). The program is seeking to attract, over 4 years, more than 150 experienced researchers to carry out research projects within the IMDEA network of research Institutes.

The program keeps a call open permanently until month 36. Applications are evaluated by batches, according to quarterly cut-off dates. To promote the program and its calls, both nationally and abroad, best practices developed during the previous AMAROUT program are being applied. The IMDEA Software Institute is the single beneficiary of the AMAROUT-II program, the same role that was performed during the previous AMAROUT program.

As in AMAROUT, the AMAROUT-II Program is a joint initiative from the seven IMDEA research institutes. The IMDEA Software Institute was in charge of writing and submitting the proposal and is the beneficiary, acting as the administrator of the program for the other institutes.

MINECO Co-Funding for AMAROUT

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2013–2015
Principal Investigator: Res. Prof. Gilles Barthe

This project awarded by MINECO funds one part of the complementary mobility costs for the researches that have been awarded fellowships within the AMAROUT II Marie Curie PEOPLE-COFUND action described above. In 2014-15 this has been extended to co-funding researchers from other IMDEA institutes within a proposal coordinated by the IMDEA Software Institute.

EIT ICT Labs CLC

Co-Location Center

The headquarters of the IMDEA Software Institute host the **Madrid Co-Location Center (CLC)** of EIT ICT Labs. The CLC is the central place for organizing and implementing EIT ICT Labs activities in Spain, and the principal meeting point for the Spanish Associate Partner Group (APG), led by IMDEA Software, which includes some of the most prominent actors in the ICT innovation arena, such as Telefónica, Indra, Atos, Technical University of Madrid (UPM) and the Barcelona Supercomputing Center (BSC).

EIT ICT Labs FI-PPP Liaison

Liaison with the Future Internet Public-Private Partnership

In 2014, IMDEA Software coordinated the activities on selecting and training startups and SMEs from the EIT ICT Labs eco-system in Spain that use FI-WARE (FI-PPP) technologies and generic enablers for developing and bringing to market innovative products and services. The public competition attracted around 40 companies, 10 of which were selected and given training in FI-WARE technologies in cooperation with *Telefonica I+D*. Finally, three finalist companies received prizes for the most innovative market solutions.

EIT ICT Labs Business Development Accelerator

This year has seen the start of the local activities of the EIT ICT Labs Business Development Accelerator (BDA), part of the EIT ICT Labs BDA network, a group of 50 specialists helping in bringing ideas to market and providing services such as coaching, access to finance, or soft landing, at a pan-European level. This has also included participation in and organization of events related to innovation and entrepreneurship such as, e.g., Spain Startup.

Microsoft Research

The strong cooperation between scientists in IMDEA Software and Microsoft Research was further boosted in 2014 through opening of the Joint Research Center and organization of the first Microsoft Research and IMDEA Software Institute Cooperation Workshop (MICW 2014). Within the Microsoft Research – IMDEA Software Joint Research Center, scientists from both sides work together on a number research topics, such as cryptography and privacy, concurrency and memory models, and programming languages and verification. The MICW has been established as an annual forum for presenting the results of the joint work.

Telefónica I+D

Since 2012, IMDEA Software has cooperated with *Telefónica I+D* on research and development in components for automatic management of cloud scalability towards their integration into *Claudia*, a product developed within the European FI-WARE initiative. *Claudia* facilitates the definition and automatic deployment and management of virtual machines, storage, and connectivity resources that comprise the virtual infrastructure on which cloud applications are run.

The Institute is in charge of providing advice on the software architecture and high-level design of the software components, within the FI-WARE requirements, and participates in their development and testing. The component integration is based on the OpenStack cloud architecture.

As mentioned before, Telefonica Digital and the Institute also established during 2013 a *Joint Research Unit* (JRU) within their more global strategic partnership.

Boeing Research & Technology Europe

IMDEA has also been contracted since 2012 by *Boeing Research & Technology Europe* (which is located in Spain), to work jointly in research and development in the fields of Big Data and Social Network Analytics. In particular, the Institute and Boeing are jointly designing and implementing a framework for data mining in social media. The framework includes a declarative embedded language designed by IMDEA Software. This language supports the description of workflows that integrate map-reduce jobs and native applications. The implementation avoids costly recomputations increasing the efficiency of social media processing, with applications in rich Web interfaces that rely on live collection of social network information from Twitter streams and other sources.

LogicBlox

In 2013, the IMDEA Software Institute started cooperation with LogicBlox, located in Georgia, USA, applying IMDEA's expertise in logic engines within the LogicBlox commercial deductive (smart) database system. The smart database and its high-level declarative query language (LogiQL) enable users used to build applications that combine transactional, analytical, graph, probabilistic, and mathematical programming. This makes possible new classes of hybrid applications that are hard or impossible to build on a traditional technological stacks that involve a cocktail of multiple programming languages and databases. This system includes sophisticated logic for optimizing database query execution, and is able to take advantage of multi-core and cloud programming, while abstracting away much of their intrinsic complexity.

Projects with Associated Groups

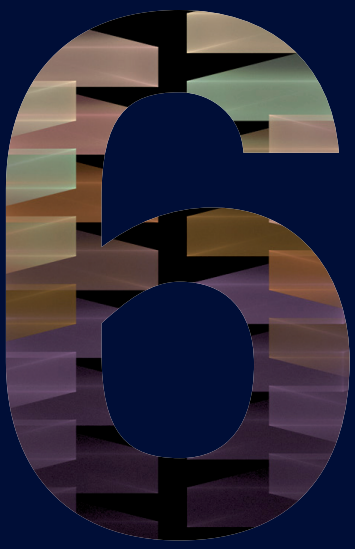
Part of the research of the Institute is performed in collaboration with research groups at associated institutions. This is exemplified by the existence of research projects led by these institutions but in which IMDEA personnel take part (and the resulting joint publications and results). We provide a summary list of the most relevant such projects which were active during 2014.

Project	Duration	Description	Funding Agency
DOVES	2009-2014	Development of verifiable and efficient software	MINECO
SpaRCIM	2003-2014	Spanish Research Consortium for Informatics and Mathematics	European Union / MINECO

5.2. Fellowships

1. *Microsoft Research PhD Scholarship funds* (2), active in 2012-2015 (**Alexey Gotsman** and **Boris Köpf**).
2. *Juan de la Cierva Postdoc grant*, Spanish Ministry of Science and Innovation, awarded in 2011 and ending in 2014 (**Juan Caballero**).
3. *Ramón y Cajal grant*, Spanish Ministry of Science and Innovation, awarded in 2010 and ending in 2015 (**Aleksandar Nanevski**).
4. *Marie Curie AMAROUT II Incoming Fellowships (8)*, European Union – 7 Framework Program, awarded in 2012 and active in 2014 (**Dario Fiore**, **Michael Emmi**, **François Dupressoir**, **Benedikt Schmidt**, **Pierre-Yves Strub Ilya Sergey**, **Giovanni Bernardi** and **Alessandra Gorla**).
5. *FPI Doctoral Grant* (2), Spanish Ministry of Science and Innovation, active in 2014 (**Juan Manuel Crespo** and **Miriam Garcia**).
6. *FPU Doctoral Grant*, Spanish Ministry of Education, Culture and Sports, awarded in 2012 and active through 2016 (**Julian Samborski-Forlese**).

dissemination of results



6.1. **Publications** **[76]**

- 6.1.1. Refereed Publications [76]
- 6.1.2. Articles in Books and other Collections [82]
- 6.1.3. Edited Volumes [82]
- 6.1.4. Doctoral and Master Theses [82]

6.2. **Invited Talks** **[83]**

- 6.2.1. Invited and Plenary Talks by IMDEA Scientists [83]
- 6.2.2. Invited Seminars and Lectures by IMDEA Scientists [84]
- 6.2.3. Invited Speaker Series [84]
- 6.2.4. Software Seminar Series [86]

6.3. **Scientific Service and Other Activities** **[87]**

- 6.3.1. Participation in Program Committees [87]
- 6.3.2. Conference and Program Committee Chairmanships [89]
- 6.3.3. Editorial Boards and Conference Steering Committees [90]
- 6.3.4. Association and Organization Committees [90]

6.4. **Awards** **[91]**

annual report 2014

6.1. Publications

6.1.1. Refereed Publications

Journals

1. *Gilles Barthe*, Delphine Demange, David Pichardie. Formal Verification of an SSA-Based Middle-End for CompCert. ACM Trans. Program. Lang. Syst., Vol. 36, Num. 1, pages 1–35, ACM, March 2014.

2. *John P. Gallagher* and Bishoksan Kafle. Analysis and Transformation Tools for Constrained Horn Clause Verification. Theory and Practice of Logic Programming, Vol. 14, Num. 4-5 (supplementary materials), pages 90–101, Cambridge University Press, 2014.

3. *Álvaro García-Pérez*, Pablo Nogueira. On the syntactic and functional correspondence between hybrid (or layered) normalisers and abstract machines. Science of Computer Programming, Vol. 95, pages 176–199, Elsevier, 2014.

4. *Alexander Malkis*, *Anindya Banerjee*. On Automation in the Verification of Software Barriers: Experience Report. J. Autom. Reasoning, Vol. 52, Num. 3, pages 275–329, 2014.

5. Laura Bozzelli, *César Sánchez*. Visibly Rational Expressions. Acta Informatica, Vol. 51, Num. 1, pages 25–49, 2014.

6. G.J. Duck, *Rémy Haemmerlé*, M. Sulzmann. On Termination, Confluence and Consistent CHR-based Type Inference. Theory and Practice of Logic Programming, 30th Int'l. Conference on Logic Programming (ICLP'14) Special Issue, Vol. 14, Num. 4-5, pages 619–632, Cambridge U. Press, 2014.

7. *Alejandro Serrano*, *Pedro Lopez-Garcia*, *Manuel Hermenegildo*. Resource Usage Analysis of Logic Programs via Abstract Interpretation Using Sized Types. Theory and Practice of Logic Programming, 30th Int'l. Conference on Logic Programming (ICLP'14) Special Issue, Vol. 14, Num. 4-5, pages 739–754, Cambridge U. Press, 2014.

8. Michel Abdalla, Dario Catalano, *Dario Fiore*. Verifiable Random Functions: Relations to Identity-Based Key-Encapsulation and New Constructions. Journal of Cryptology, Vol. 27, Num. 3, pages 544–593, Springer, 2014.

9. *François Dupressoir*, Andrew D. Gordon, Jan Jürjens, David A. Naumann. Guiding a general-purpose C verifier to prove cryptographic protocols. Journal of Computer Security, Vol. 22, Num. 5, pages 823–866, 2014.

10. *Guillermo Vigueras*, Ishani Roy, Andrew Cookson, Jack Lee, Nicolas Smith, David Nordsletten. Toward GPGPU accelerated human electromechanical cardiac simulations. International Journal for Numerical Methods in Biomedical Engineering, Vol. 30, Num. 1, pages 117–134, 2014.

11. *Guillermo Vigueras*, Juan M. Orduña, Miguel Lozano, Jose M. Cecilia, Jose M. Garcia. Accelerating collision detection for large-scale crowd simulation on multi-core and many-core architectures. International Journal of High Performance Computing and Applications, Vol. 28, Num. 1, 2014.

12. J. Ian Johnson, *Ilya Sergey*, Christopher Earl, Matthew Might, David Van Horn. Pushdown flow analysis with abstract garbage collection. J. Funct. Program., Vol. 24, Num. 2-3, pages 218–283, 2014.

13. Ahmed Bouajjani, *Michael Emmi*. Bounded phase analysis of message-passing programs. STTT, Vol. 16, Num. 2, pages 127–146, 2014.

14. David A. Basin, *Manuel Clavel*, Marina Egea, *Miguel Ángel García de Dios*, *Carolina Dania*. A Model-Driven Methodology for Developing Secure Data-Management Applications. IEEE Trans. Software Eng., Vol. 40, Num. 4, pages 324–337, 2014.

15. Javier Esparza, *Pierre Ganty*, Tomás Poch. Pattern-based Verification for Multithreaded Programs. ACM Transactions on Programming Languages and Systems, Vol. 36, Num. 3, pages 1–29, 2014.

publications

Conferences

1. *M. Zubair Rafique*, *Juan Caballero*, Christophe Huygens, Wouter Joosen. Network Dialog Minimization and Network Dialog Diffing: Two Novel Primitives for Network Security Applications. Proceedings of the 2014 Annual Computer Security Applications Conference, December 2014.

2. *Gilles Barthe*, Gustavo Betarte, Juan Diego Campo, Carlos Luna, David Pichardie. System-level non-interference for constant-time cryptography. 21st ACM Conference on Computer and Communications Security (CCS 2014), November 2014. IACR Cryptology ePrint Archive, Report 2014/422, pages 1267–1279, ACM, November 2014.

3. *Gilles Barthe*, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, Jean-Christophe Zapalowicz.Synthesis of Fault Attacks on Cryptographic Implementations. 21st ACM Conference on Computer and Communications Security (CCS 2014), November 2014. IACR Cryptology ePrint Archive, Report 2014/436, pages 1016–1027. ACM Press, New York, NY, USA, 2014.

4. *Dragan Ivanović*, *Manuel Carro*. Transforming Service Compositions into Cloud-Friendly Actor Networks. Service-Oriented Computing - 12th International Conference, ICSOC 2014, Paris, France, November 3-6, 2014. Proceedings, LNCS, Vol. 8831, pages 291–305, Springer Verlag, November 2014.

5. *Dragan Ivanović*, *Manuel Carro*, Peerachai Kaowichakorn. Towards QoS Prediction Based on Composition Structure Analysis and Probabilistic Models. Service-Oriented Computing - 12th International Conference, ICSOC, LNCS, Vol. 8831, pages 394–402, Springer Verlag, November 2014.

6. Zhaoyan Xu, *Antonio Nappa*, Robert Baykov, Guangliang Yang, Juan Caballero, Guofei Gu. AutoProbe: Towards Automatic Active Malicious Server Probing Using Dynamic Binary Analysis. Proceedings of the 21st ACM Conference on Computer and Communication Security, November 2014.

7. Liang Wang, *Antonio Nappa*, *Juan Caballero*, Thomas Ristenpart, Aditya Akella. WhoWas: A Platform for Measuring Web Deployments on IaaS Clouds. Proceedings of the 2014 ACM Internet Measurement Conference, November 2014.

8. *Remy Haemmerlé*. On Combining Backward and Forward Chaining in Constraint Logic Programming. 16th Int'l. ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'14), 12 pages, ACM Press, September 2014.

9. *Jose Francisco Morales*, *Manuel Hermenegildo*. Pre-Indexed Terms for Prolog. Pre-proceedings of the 24th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'14), 15 pages, September 2014.

10. *Nataliia Stulova*, *Jose Francisco Morales*, *Manuel Hermenegildo*. Assertion-based Debugging of Higher-Order (C)LP Programs. 16th Int'l. ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'14), 15 pages, ACM Press, September 2014.

11. David Urbina, Yufei Gu, *Juan Caballero*, Zhiqiang Lin. SigPath: A Memory Graph Based Approach for Program Data Introspection and Modification. Proceedings of the 19th European Symposium on Research in Computer Security, September 2014.

12. Joseph A. Akinyele, *Gilles Barthe*, Benjamin Grégoire, *Benedikt Schmidt*, *Pierre-Yves Strub*. Certified Synthesis of Efficient Batch Verifiers. Computer Security Foundations Symposium (CSF 2014), July 2014.

13. *Gilles Barthe*, Marco Gaboardi, Emilio Jesús Gallego Arias, Justin Hsu, César Kunz, *Pierre-Yves Strub*. Proving differential privacy in Hoare logic. Computer Security Foundations Symposium (CSF 2014), July 2014. CoRR abs/1407.2988 [cs.LO].

14. *Nataliia Stulova*, *Jose Francisco Morales*, *Manuel Hermenegildo*. Towards Assertion-based Debugging of Higher-Order (C)LP Programs (Extended Abstract). Theory and Practice of Logic Programming, 30th Int'l. Conference on Logic Programming (ICLP'14) Special Issue, On-line Supplement, Cambridge U. Press, July 2014.

15. *Antonio Nappa*, Zhaoyan Xu, *Juan Caballero*, Guofei Gu. CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers. Proceedings of the Network and Distributed System Security Symposium, February 2014.

16. Hagit Attiya, *Alexey Gotsman*, Sandeep Hans, Noam Rinetzky. Safety of live transactions in transactional memory: TMS is necessary and sufficient. DISC'14: International Symposium on Distributed Computing, Austin, TX, USA, LNCS, Vol. 8784, pages 376–390, Springer, 2014.

17. *Andrea Cerone*, *Alexey Gotsman*, Hongseok Yang. Parameterised linearisability. ICALP'14: International Colloquium on Automata, Languages, and Programming, Copenhagen, Denmark, LNCS, Vol. 8573, pages 271–284, Springer, 2014.

18. *Andrea Cerone*, Matthew Hennessy. Characterising Testing Preorders for Broadcasting Distributed Systems. Trustworthy Global Computing - 9th International Symposium, (TGC) 2014, Rome, Italy, September 5-6, 2014. Revised Selected Papers. LNCS Volume 8902, pages 67–81. Springer, 2014.

19. Sebastian Burckhardt, *Alexey Gotsman*, Hongseok Yang, Marek Zawirski. Replicated data types: specification, verification, optimality. Proceedings of the 41st ACM Symposium on Principles of Programming Languages (POPL'14), San Diego, CA, USA, pages 271–284, ACM Press, 2014.

20. *Álvaro García-Pérez*, Pablo Nogueira, *Ilya Sergey*. Deriving Interpretations of the Gradually-Typed Lambda Calculus. Proceedings of the ACM SIGPLAN 2014 Workshop on Partial Evaluation and Program Manipulation, PEPM '14, pages 157–168, ACM, 2014.

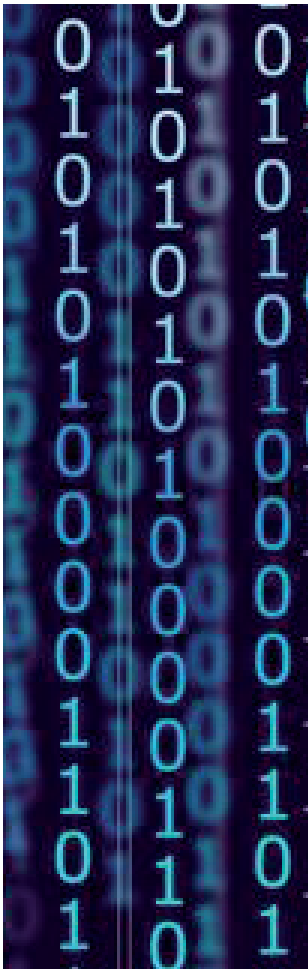
21. Shachar Itzhaky, *Anindya Banerjee*, Neil Immerman, Ori Lahav, *Aleksandar Nanevski*, Mooly Sagiv. Modular reasoning about heap paths via effectively propositional formulas. The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014, pages 385–396, 2014.

22. *Anindya Banerjee*, David A. Naumann. A Logical Analysis of Framing for Specifications with Pure Method Calls. Verified Software: Theories, Tools and Experiments - 6th International Conference, VSTTE 2014, Vienna, Austria, July 17-18, 2014, Revised Selected Papers, pages 3–20, 2014.

23. *Gilles Barthe*, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, Mehdi Tibouchi, Jean-Christophe Zapalowicz. Making RSA-PSS Provably Secure against Non-random Faults. Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings, Lecture Notes in Computer Science, Vol. 8731, pages 206–222, Springer, 2014.

24. *Gilles Barthe*, *Edvard Fagerholm*, *Dario Fiore*, John C. Mitchell, Andre Scedrov, *Benedikt Schmidt*. Automated Analysis of Cryptographic Assumptions in Generic Group Models. Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 8616, pages 95–112, Springer, 2014.

25. *Gilles Barthe*, Cédric Fournet, Benjamin Grégoire, *Pierre-Yves Strub*, Nikhil Swamy, Santiago Zanella Béguelin. Probabilistic relational verification for cryptographic implementations. The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014, pages 193–206, ACM, 2014.



26. *Gilles Barthe*, *Boris Köpf*, Laurent Mauborgne, Martín Ochoa. Leakage Resilience against Concurrent Cache Attacks. Principles of Security and Trust - Third International Conference, POST 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014, Proceedings, Lecture Notes in Computer Science, Vol. 8414, pages 140–158, Springer, 2014.

27. *Gilles Barthe*, Marco Gaboardi, Emilio Jesús Gallego Arias, Justin Hsu, Aaron Roth, Pierre-Yves Strub. Higher-Order Approximate Relational Refinement Types for Mechanism Design and Differential Privacy. Computer Security Foundations Symposium (CSF 2014), 2014. CoRR abs/1407.6845 [cs.PL].

28. *Pavithra Prabhakar*, *Miriam Garcia Soto*. Foundations of Quantitative Predicate Abstraction for Stability Analysis of Hybrid Systems. Verification, Model-Checking and Abstract Interpretation (VMCAI), 2015.

29. Scott C. Livingston, *Pavithra Prabhakar*. Decoupled formal synthesis for almost separable systems with temporal logic specifications. International Symposium on Distributed Autonomous Robotic Systems (DARS), 2014.

30. Jun Liu and *Pavithra Prabhakar*. Switching Control of Dynamical Systems from Metric Temporal Logic Specifications. IEEE International Conference on Robotics and Automation (ICRA), 2014.

31. *Pavithra Prabhakar*, *Miriam García Soto*. An algorithmic approach to stability verification of polyhedral switched systems. American Control Conference (ACC), 2014.

32. *Benedikt Schmidt*, Ralf Sasse, Cas Cremers, David Basin. Automated Verification of Group Key Agreement Protocols. Proceedings of the 2014 IEEE Symposium on Security and Privacy, SP '14, pages 179–194, IEEE Computer Society, 2014.

33. *Alejandro Sánchez*, *César Sánchez*. Formal Verification of Skiplists with Arbitrarily Many Levels. Proc. of the 12th Int'l Symp. on Automated Technology for Verification and Analysis (ATVA), LNCS, Springer, 2014.

34. *Alejandro Sánchez*, *César Sánchez*. Parametrized Verification Diagram. Proc. of the 21st Int'l Symp. on Temporal Representation and Reasoning (TIME'14), IEEE Computer Society Press, 2014.

35. Laura Bozzelli, *César Sánchez*. Foundations of Boolean Stream Runtime Verification. Proceedings of the 14th International Conference on Runtime Verification (RV'14). LNCS, Vol. 8734, pages 64–79, Springer, 2014.

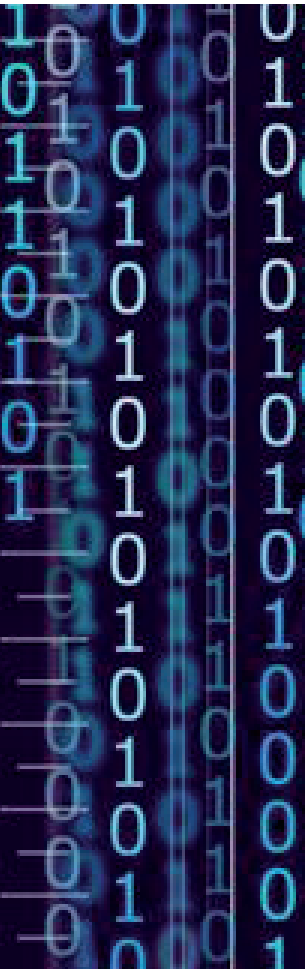
36. Laura Bozzelli, *César Sánchez*. Visibly Linear Temporal Logic. Proc. of the 7th Int'l Joint Conf. on Automated Reasoning (IJCAR'14), LNCS, Vol. 8562, pages 418–433, Springer, 2014.

37. *Umer Liqat*, S. Kerrison, *Alejandro Serrano*, K. Georgiou, P. Lopez-Garcia, N. Grech, M.V. Hermenegildo, K. Eder. Energy Consumption Analysis of Programs based on XMOS ISA-Level Models. Proceedings of the 23rd International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'13), 2014.

38. *Dario Fiore*, Rosario Gennaro, Valerio Pastro. Efficiently Verifiable Computation on Encrypted Data. ACM CCS 2014 – 21th ACM Conference on Computer and Communication Security, pages 844–855, 2014.

39. Dario Catalano, *Dario Fiore*, Bogdan Warinschi. Homomorphic Signatures with Efficient Verification for Polynomial Functions. Advances in Cryptology – CRYPTO 2014 – 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I, LNCS, Vol. 8616, pages 371–389, Springer, 2014.

40. Dario Catalano, *Dario Fiore*, Rosario Gennaro, *Luca Nizzardo*. Generalizing Homomorphic MACs for Arithmetic Circuits. PKC 2014: 17th International Workshop on Theory and Practice in Public Key Cryptography, LNCS, Vol. 8383, pages 538–555, Springer, 2014.



41. Yevgeniy Dodis, *Dario Fiore*. Interactive Encryption and Message Authentication. Security and Cryptography for Networks - 9th International Conference, SCN 2014, LNCS, Vol. 8642, pages 494–513, Springer, 2014.

42. *Giovanni Bernardi*, Ornela Dardha, Simon J. Gay, Dimitrios Kouzapas. On Duality Relations for Session Types. Trustworthy Global Computing, TGC 2014 Revised Selected Papers, Lecture Notes in Computer Science, pages 51–66, Springer Berlin Heidelberg, 2014.

43. *Giovanni Bernardi*, Matthew Hennessy. Using Higher-Order Contracts to Model Session Types (Extended Abstract). CONCUR 2014 - Concurrency Theory - 25th International Conference, CONCUR 2014, Rome, Italy, September 2-5, 2014. Proceedings, Lecture Notes in Computer Science, Vol. 8704, pages 387–401, Springer, 2014.

44. *Aleksandar Nanevski*, Ruy Ley-Wild, *Ilya Sergey*, *Germán Andrés Delbianco*. Communicating State Transition Systems for Fine-Grained Concurrent Resources. Proceedings of the 23rd European Symposium on Programming, ESOP 2014, LNCS, pages 290–310, Springer, 2014.

45. *Ilya Sergey*, Dimitrios Vytiniotis, Simon L. Peyton Jones. Modular, higher-order cardinality analysis in theory and practice. Proceedings of the 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, pages 335–348, ACM, 2014.

46. *Alejandro Sánchez*, *César Sánchez*. LEAP: A Tool for the Parametrized Verification of Concurrent Datatypes. Proc. of the 26th Int'l Conf. on Computer Aided Verification (CAV'14), Vienna, Austria, July 18-22, 2014. LNCS, Vol. 8559, pages 620–627, Springer, 2014.

47. Zvonimir Rakamaric, *Michael Emmi*. SMACK: Decoupling Source Language Details from Verifier Implementations. Computer Aided Verification - 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. LNCS, Vol. 8559, pages 106–113, Springer, 2014.

48. *Michael Emmi*, Burcu Kulahcioglu Ozkan, Serdar Tasiran. Exploiting synchronization in the analysis of shared-memory asynchronous programs. 2014 International Symposium on Model Checking of Software, SPIN 2014, Proceedings, San Jose, CA, USA, July 21-23, 2014, pages 20–29, ACM, 2014.

49. *Carolina Dania*, *Manuel Clavel*. Modeling Social Networking Privacy. 2014 Theoretical Aspects of Software Engineering Conference, TASE 2014, Changsha, China, September 1-3, 2014, pages 50–57, 2014.

50. *Pierre Ganty*, Ahmed Rezine. Ordered Counter Abstraction (Refinable Subword Relations for Parameterized Verification). LATA'14, 8th Int. Conf. on Language and Automata Theory and Applications, LATA'14, March 10-14, Madrid, Spain. LNCS, Vol. 8370, pages 396-407, Springer, 2014.

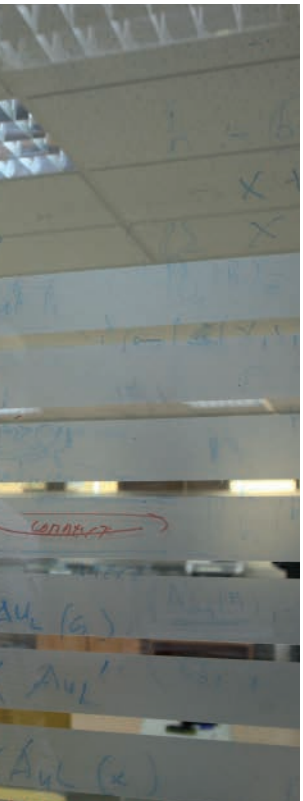
51. Karthikeyan Bhargavan, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, *Pierre-Yves Strub*, Santiago Zanella Béguelin. Proving the TLS Handshake Secure (As It Is). Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II, pages 235–255, 2014.

52. Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Alfredo Pironti, *Pierre-Yves Strub*. Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS. Proceedings of the 2014 IEEE Symposium on Security and Privacy, SP '14, pages 98–113, IEEE Computer Society, 2014.

53. Evmorfia-Iro Bartzia, *Pierre-Yves Strub*. A Formal Library for Elliptic Curves in the Coq Proof Assistant. Interactive Theorem Proving - 5th International Conference, ITP 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings, Lecture Notes in Computer Science, Vol. 8558, pages 77–92, Springer, 2014.

54. Nikhil Swamy, Cédric Fournet, Aseem Rastogi, Karthikeyan Bhargavan, Juan Chen, *Pierre-Yves Strub*, Gavin M. Bierman. Gradual typing embedded securely in JavaScript. The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014, pages 425–438, ACM, 2014.

55. *Zhoulai Fu*. Targeted Update - Aggressive Memory Abstraction Beyond Common Sense and Its Application on Static Numeric Analysis. Programming Languages and Systems - 23rd European Symposium on Programming, ESOP 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014, Proceedings, pages 534–553, 2014.



Workshops

1. Marcos Arjona, *Carolina Dania*, Marina Egea, Antonio Maña. Validation of a Security Metamodel for the Development of Cloud Applications. Proceedings of the 14th International Workshop on OCL and Textual Modelling co-located with 17th International Conference on Model Driven Engineering Languages and Systems (MODELS 2014), Valencia, Spain, September 30, 2014., pages 33–42, 2014.

2. Achim D. Brucker, Tony Clark, *Carolina Dania*, Geri Georg, Martin Gogolla, Frédéric Jouault, Ernest Teniente, Burkhart Wolff. Panel Discussion: Proposals for Improving OCL. Proceedings of the 14th International Workshop on OCL and Textual Modelling co-located with 17th International Conference on Model Driven Engineering Languages and Systems (MODELS 2014), Valencia, Spain, September 30, 2014., pages 83–99, 2014.

3. Bishoksan Kafle, *John P. Gallagher*. Convex polyhedral abstractions, specialisation and property-based predicate splitting in Horn clause verification. Proceedings First Workshop on Horn Clauses for Verification and Synthesis, HCVS 2014, Vienna, Austria, 17 July 2014, Vol. 169, pages 53–67, EPTCS, 2014.

4. *Jose Francisco Morales*, *Manuel Hermenegildo*. Towards Pre-Indexed Terms. 14th International Colloquium on Implementation of Constraint and LOgic Programming Systems (CICLOPS-WLPE 2014), 14 pages, RWTH Aachen University, July 2014.

6.1.2. Articles in Books and other Collections

1. K. Georgiou, *Umer Liqat*, *Pedro Lopez-Garcia*, *Manuel Hermenegildo*, K. Eder. Towards LLVM-Based Energy Consumption Analysis of Programs. ICT-Energy (Nanoenergy) Letters, Num. 8, July 2014.

2. *Miguel Ángel García de Dios*, *Carolina Dania*, David A. Basin, *Manuel Clavel*. Model-Driven Development of a Secure eHealth Application. Engineering Secure Future Internet Services and Systems - Current Research, pages 97–118, 2014.

6.1.3. Edited Volumes

1. *Juan Caballero*, Simson Garfinkel. Proceedings of the 14th Annual Digital Forensics Research Conference. J. of Digital Investigation, Vol. 11, Supplement 2, pages S1–S2, 2014.

2. Davide Balzarotti, *Juan Caballero*. Proceedings of the Seventh European Workshop on System Security, EuroSec 2014, April 13, 2014, Amsterdam, The Netherlands. ACM Press, 2014.

3. Achim D. Brucker, *Carolina Dania*, Geri Georg, Martin Gogolla. Proceedings of the 14th International Workshop on OCL and Textual Modelling co-located with 17th International Conference on Model Driven Engineering Languages and Systems (MODELS 2014), Valencia, Spain, September 30, 2014. CEUR Workshop Proceedings 1285, CEUR-WS.org 2014.

4. *Remy Haemmerlé*, J. Sneyers. Proceedings of the Eleventh Workshop on Constraint Handling Rules (CHR 2014). CoRR abs/1406.1510, 2014.

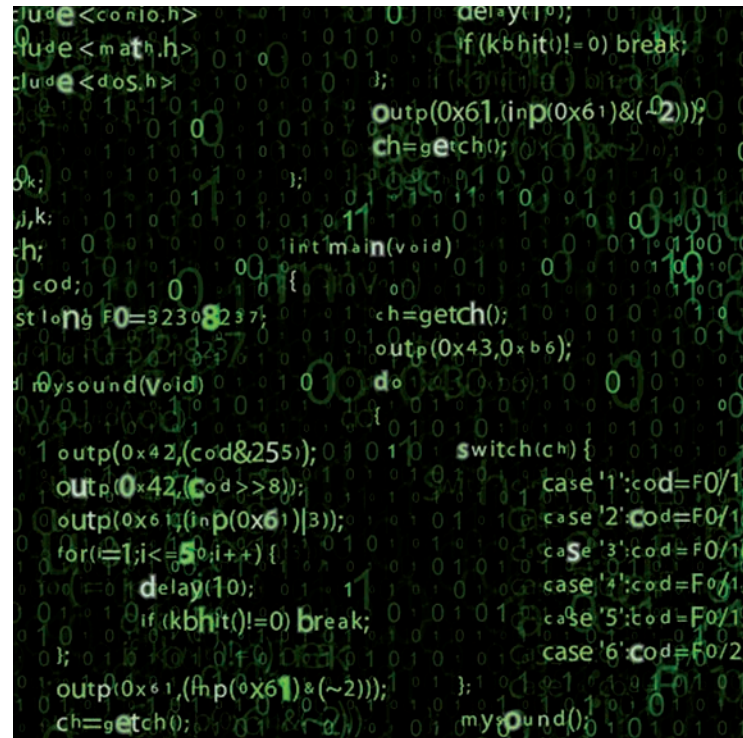
6.1.4. Doctoral and Master Theses

1. Federico Olmedo. *Approximate Relational Reasoning for Probabilistic Programs*. PhD Thesis. Technical University of Madrid (UPM). January 2014. Advisor: Gilles Barthe (IMDEA Software Institute).

2. Irfan Khan Tanoli. *An Empirical Study of Techniques to Detect Reverse Proxies and Load Balancers in HTTP Traffic*. MSc Thesis. Technical University of Madrid (UPM). June 2014. Advisor: Juan Caballero (IMDEA Software Institute).

3. Richard Rivera Guevarra. *Análisis de Características Estáticas de Ficheros Ejecutables para la Clasificación de Malware*. MSc Thesis. Technical University of Madrid (UPM). June 2014. Advisor: Juan Caballero (IMDEA Software Institute).

4. Artem Khyzha. *Concurrent Library Abstraction without Information Hiding*. MSc Thesis. Technical University of Madrid (UPM). July 2014. Advisor: Alexey Gotsman (IMDEA Software Institute).



6.2. Invited Talks

6.2.1. Invited and Plenary Talks by IMDEA Scientists

1. *Gilles Barthe*. Invited talk at the Computer Security Foundation Symposium (CSF 2014).

2. *Gilles Barthe*. Invited talk at the 11th Latin American Theoretical Informatics Symposium (LATIN 2014).

3. *Gilles Barthe*. Invited talk at the Vienna Summer of Logic workshop "All about Proofs, Proof for All" (APPA 2014).

4. *Juan Caballero*. CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers. Invited talk at Cursos de Verano de la Universidad Rey Juan Carlos, Madrid, June 2014.

5. *Juan Caballero*. Binary Type Inference. Invited talk at Dagstuhl Seminar Challenges in Analysing Executables: Scalability, Self-Modifying Code and Synergy. Schloss Dagstuhl, Germany. June 2014.

6. *Andrea Cerone*. Parameterised Linearisability. Invited talk at the York Concurrency Workshop, April 2014.

7. *François Dupressoir*. Efficient Provably Secure Machine Code from High-Level Implementations. Invited talk at the Real-World Cryptography Workshop. New York. January 2014.

8. *François Dupressoir*. Formal Adventures in the Land of Masking-Based Side-Channel Countermeasures. Dagstuhl Seminar 14492, Schloss Dagstuhl, Germany, November 2014.

9. *Pierre Ganty*. Parameterized Verification of Asynchronous Shared-Memory Systems. Invited talk at The First Workshop on Parameterized Verification, Rome, September 2014.

10. *Alessandra Gorla*. CHABADA: Checking app behavior against app descriptions. Invited talk at th 36th CREST Open Workshop, University College London, UK. November 2014.

11. *Alessandra Gorla*. Mining Android Applications for Anomalies. Dagstuhl Seminar 14261 on Software Development Analytics. July 2014.

12. *Alexey Gotsman*. Weak consistency in cloud storage. Dagstuhl seminar n. 14511 on Programming Languages for Big Data. December 2014.

13. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. York Concurrency Workshop. April 2014.

14. *Manuel Hermenegildo*. Energy Analysis, Debugging, and Verification with the CiaoPP system. In Next Generation Static Software Analysis Tools. Schloss Dagstuhl. August 2014.

15. *Juan José Moreno-Navarro*. Towards a doctorate linked with innovation and entrepreneurship. Fostering University Business Cooperation Ecosystems in Europe and Latin America. University-Business Thematic Forum, European Commission and Universidad Autonoma de Madrid. June 2014.

16. *Juan José Moreno-Navarro*. Cuidando el talento: La oferta de posgrado de la UPM y de EIT ICT Labs. Calidad, profesionalización, emprendimiento e internacionalización. FICOD 2014, September 2014.

17. *Pavithra Prabhakar*. Formal Verification of Cyber-Physical Systems. Invited talk at the Tenth International Symposium on Tools and Methods of Competitive Engineering (TMCE 2014). Budapest, Hungary. May 2014.

6.2.2. Invited Seminars and Lectures by IMDEA Scientists

1. *Giovanni Bernardi*. Dualities and testing relations for session types. Invited talk at COST Action IC1201 meeting. August 2014.

2. *Juan Caballero*. Program Data Introspection and Dynamic Type Inference of Binary Code. INRIA, Rennes. September 2014.

3. *Juan Caballero*. CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers. Invited talk at Security Seminar at Microsoft Research, Redmond. July 2014.

4. *Juan Caballero*. CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers. Invited talk at Royal Holloway University of London, London, UK. March 2014.

5. *Andrea Cerone*. Parameterised Linearisability. Invited talk at Trinity College, Dublin. May 2014.

6. *Andrea Cerone*. Parameterised Linearisability. Invited talk at Aarhus University. June 2014.

7. *Manuel Clavel*. Model-driven engineering in action. Lecture at the Industrial University of Ho Chi Minh City, Vietnam. January–February 2014.

8. *Carolina Dania*. Analysis of OCL properties on static and dynamic UML models. Saarland University, Saarbrucken, Germany. July 2014.

9. *Germán Del Bianco*. Concurrent Hoare Style Reasoning, Deconstructed. SELEN Seminar Series. Department of Computer Science, National University of Rosario. Rosario, Argentina. November 2014.

10. *Dario Fiore*. Verifiable Delegation of Computation on Outsourced Data. Universidad Rey Juan Carlos. Madrid, May 2014.

11. *Dario Fiore*. Verifiable Delegation of Computation on Outsourced Data. Universidad de la Republica, Montevideo, Uruguay. March 2014.

12. *Alvaro García*. Reasoning about structural operational semantics in a calculus of closures. ICE-TCS seminar, School of Computer Science, Reykjavík University, April 2014.

13. *Alessandra Gorla*. Checking App Behavior Against App Descriptions. University of Uruguay. August 2014.

14. *Alessandra Gorla*. Checking App Behavior Against App Descriptions. University of Luxembourg. May 2014.

15. *Alexey Gotsman*. Formalizing isolation guarantees of modern replicated databases. Invited talk at University of California at Berkeley. August 2014.

16. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. Invited talk at Universidade do Minho, Portugal. March 2014.

17. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. Invited talk at Aachen University, Germany. March 2014.

18. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. Invited talk at Universidad Nova Lisboa, Portugal. June 2014.

19. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. Invited talk at University of Paris 6, France. September 2014.

20. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. Invited talk at University of California at Los Angeles. August 2014.

21. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. Invited talk at University of Washington. August 2014.

22. *Alexey Gotsman*. Reasoning about Eventual Consistency and Replicated Data Types. Invited talk at University of Utah. August 2014.

23. *Manuel Hermenegildo*. Abstract Interpretation-based Energy Analysis, Debugging, and Verification. Invited talk at the Energy Aware COmputing Workshop, Bristol. September 2014.

24. *Boris Koepf*. Static Analysis of Cache Side Channels. Invited talk at EPF Lausanne, Processor Architecture Lab. April 2014.

25. *Boris Koepf*. Managing the Trade-off between Security and Performance. Invited talk at the RISK seminar. ETH Zurich. November 2014.

26. *Boris Koepf*. Static Analysis of Cache Side Channels. Invited talk at TU Darmstadt. December 2014

27. *Antonio Nappa*. Rubik: The Multiple Facets of Cybercrime. CyberCamp, Madrid. December 2014.

28. *Pavithra Prabhakar*. Algorithmic Verification of Stability of Hybrid Systems. Invited talk at the RiSE seminar series. IST Austria & TU Wien. November 2014.

29. *Pavithra Prabhakar*. Formal Verification of Cyber-Physical Systems.Invited talk at Galois, Inc, Portland, USA. June 2014.

30. *Ilya Sergey*. Formal Mathematics as a Branch of Computer Science. Sociological Institute of the Russian Academy of Sciences. Saint Petersburg, Russia. August 2014.

6.2.3. Invited Speaker Series

During 2014, 23 external speakers were invited to give talks at IMDEA Software. The following list gives the speakers and the titles of their talks.

1. *Carmela Troncoso*. Post-doctoral Researcher, Gradiant, Spain: Bayesian inference to evaluate information leakage in complex scenarios.

2. *Giovanni Bernardi*. PhD Student, Trinity College, Dublin, Ireland: Using higher-order contracts to model session types.

3. *Laura Titolo*. PhD Student, University of Udine, Italy: An Abstract Interpretation Framework for Diagnosis and Verification of Timed Concurrent Constraint Languages.

4. *Chris Parnin*. PhD Student, Georgia Institute of Technology, USA: Programmer, Interrupted.

5. *Julia Rubin*. Researcher, Haifa Research Lab: To Merge or Not to Merge: Managing Software Families.

6. *Domenico Bianculli*. Researcher, Università della Svizzera Italiana, Lugano, Switzerland: A Journey through Specification and Verification Techniques for Open-World Software.

7. *Hazem Torfah*. PhD Student, Saarland University, Germany: Counting Models of Linear-time Temporal Logic.

8. *Giordano Tamburelli*. PhD Student, Università della Svizzera Italiana, Lugano, Switzerland: Models at run-time: open challenges and existing solutions.

9. *Alessandra Gorla*. Post-doctoral Researcher, Saarland University, Germany: Improving the reliability of software systems using their intrinsic redundancy.

10. *June Andronick*. Senior Research Engineer, NICTA, Australia: Trustworthy Systems at NICTA.

11. *June Andronick*. Senior Research Engineer, NICTA, Australia: Formal proof of security for million-lines-of-code systems.

12. *Jim Kapinski*. Senior Research Engineer, Toyota Technical Center, Los Angeles, USA: Simulation-Guided Analysis for Industrial Embedded Control Designs.

13. *Colin Fleming*: Cursive – an IDE for Clojure Programming Language.

14. *Deepak Kapur*. Research Professor, University of New Mexico, USA: A Quantifier-Elimination Heuristic for Octagonal Constraints.

15. *Somesh Jha*. Professor, University of Wiscounsin, USA: Retrofitting Legacy Code for Security.

16. *Mihir Bellare*. Professor, UC San Diego, USA: Caught between Theory and Practice.

17. *Jan Midtgaard*. Post-doctoral Researcher, Aarhus University, Denmark: QuickChecking Static Analysis Properties.

18. *Hongseok Yang*. Professor, University of Oxford, UK: How to find a good program abstraction automatically?

19. *Amir Ben-Amram*. Professor, Tel Aviv-Yaffo Academic College: What is decidable in growth-rate analysis of programs?

20. *Dimitrios Vytiniotis*. Researcher, Microsoft Research, Cambridge, UK: Ziria: wireless programming for hardware dummies.

21. *Michael Näf*: The Doodle Story.

22. *Roberto Giacobazzi*, Faculty (visiting), IMDEA Software Institute: Obscuring code - Unveiling and Veiling Information in Programs.

23. *Darko Stefanovic*. Associate Professor, University of New Mexico, USA: Playing robotics with DNA.

6.2.4. Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of **17** seminars were given in 2014.

6.3. Scientific Service and Other Activities

6.3.1. Participation in Program Committees

Zorana Bankovic:

1. Genetic and Evolutionary Computation Conference (GECCO 2014). Real World Applications track.

2. 10th IFIP International Conference on Artificial Intelligence Applications and Innovations (AIAI 2014).

Gilles Barthe:

3. 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2014).

4. Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL 2014) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2014).

Juan Caballero:

5. 35th IEEE Symposium on Security & Privacy (IEEE S&P 2014).

6. 36th International Conference on Software Engineering – New Ideas and Emerging Results Track (NIER-ICSE 2014).

7. 2014 Network and Distributed System Security Symposium (NDSS 2014).

Manuel Carro:

8. XIV Jornadas de PROgramación y LEnguajes (PROLE 2014).

9. 12th International Conference on Service-Oriented Computing (ICSOC 2014)

Manuel Clavel:

10. 14th International Workshop on OCL and Textual Modeling Applications and Case Studies (OCL 2014).

11. European Conference on Modeling Foundations and Applications (ECMFA 2014).

12. 10th International Workshop on Rewriting Logic and its Applications (WRLA 2014).

Carolina Dania:

13. 14th International Workshop on OCL and Textual Modeling Applications and Case Studies (OCL 2014).

Francois Dupressoir:

14. Workshop on Security Proofs for Embedded Systems (PROOFS 2014).

Dario Fiore:

15. 9th Conference on Security and Cryptography for Networks (SCN 2014).

16. 7th International Conference on Cryptology (Africacrypt 2014).

17. 2nd Workshop on Applied Homomorphic Cryptography and Encrypted Computing (WAHC 2014).

John Gallagher:

18. First Workshop on Horn Clauses for Verification and Synthesis (HCVS 2014).

19. Workshop on Logic-based methods in Programming Environments of the International Colloquium on Implementation of Constraint and LOgic Programming Systems (CICLOPS-WLPE 2014).

20. Twelfth International Symposium on Functional and Logic Programming (FLOPS 2014).

Pierre Ganty:

21. 41st International Colloquium on Automata, Languages and Programming (ICALP 2014).

22. 12th International Symposium on Automated Technology for Verification and Analysis (ATVA 2014).

Alessandra Gorla:

23. The 22nd ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2014). Artifact Evaluation committee member.

24. International Symposium on Software Testing and Analysis (ISSTA 2014). Artifact Evaluation committee member.

25. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2014), Posters track.

Alexey Gotsman:

26. The 18th International Conference on Principles of Distributed Systems (OPODIS 2014).

Rémy Haemmerlé:

27. 30th International Conference on Logic Programming (ICLP 2014).

Manuel Hermenegildo:

28. 16th International Symposium on Practical Aspects of Declarative Languages (PADL 2014).

29. 10th European Computer Science Summit (ECSS 2014).

Dragan Ivanovic

30. 11th Workshop on Constraint Handling Rules (CHR 2014).

31. 6th International Workshop on Principles of Engineering Service-Oriented Systems (PESOS 2014).

Boris Koepf:

32. 27th IEEE Computer Security Foundations Symposium (CSF 2014).

33. 11th International Conference on Quantitative Evaluation of Systems (QEST 2014).

34. 9th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS 2014).

35. 9th International Symposium on Trustworthy Global Computing (TGC 2014).

José Morales:

36. 30th International Conference on Logic Programming (ICLP 2014).

37. International Conference on Logic Programming (ICLP) Doctoral Consortium 2014.

Juan José Moreno:

38. XIV Jornadas sobre Programacion y Lenguajes (PROLE 2014).

39. XIX edicion de las Jornadas de Ingenieria del Software y Bases de Datos (JISBD 2014).

40. X Jornadas de Ciencia e Ingenieria de Servicios (JCIS 2014).

Pavithra Prabhakar:

41. 26th International Conference on Computer Aided Verification (CAV 2014).

42. 17th ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2014).

43. ACM SIGBED Summer Simulation Conference (SummerSim 2014).

César Sánchez:

44. The 8th International Symposium on Theoretical Aspects of Software Engineering (TASE 2014).

45. 5th International Symposium on Games, Automata, Logics and Formal Verification (GandALF 2014).

46. 1st workshop on Logics and Model Checking for Self*-systems (MOD* 2014).

47. 7th International Workshop on Harnessing Theories for Tool Support in Software (TTSS 2014).

Ilya Sergey:

48. 16th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014).

49. 5th Annual Scala Workshop (Scala 2014).

50. European Conference on Object-Oriented Programming (ECOOP 2014), Artifact Evaluation Committee.

Pierre-Yves Strub:

51. Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC 2014).

52. 3rd International Workshop on Confluence (IWC 2014).

6.3.2. Conference and Program Committee Chairmanship

Juan Caballero:

1. TPC Chair for the 14th Annual Digital Forensics Research Conference (DFRWS 2014).

2. TPC Co-chair for the 7th European Workshop on Systems Security (EuroSec 2014).

Manuel Carro:

3. General chair of the 30th International Conference on Logic Programming (ICLP 2014).

Michael Emmi:

4. Program Co-chair of the 7th International Workshop on Exploiting Concurrency Efficiently and Correctly (EC2 2014).

Rémy Haemmerlé:

5. Program chair of the 11th International Workshop on Constraint Handling Rules (CHR 2014).

Boris Koepf:

6. PC Co-chair for the Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC 2014).

6.3.3. Editorial Boards and Conference Steering Committees

Gilles Barthe:

1. Editorial board of the Journal of Automated Reasoning.

2. Editorial board of the Journal of Computer Security.

3. Steering committee of Principles of Security and Trust (POST).

4. Steering committee of the European Joint Conferences on Theory and Practice of Software (ETAPS).

5. Steering committee of Trustworthy Global Computing (TGC).

Manuel Carro:

6. Conference Coordinator of the Association for Logic Programming (ALP).

John Gallagher:

7. Editorial board of Theory and Practice of Logic Programming (Cambridge Univ. Press). Area Editor for Technical Notes and Rapid Publications.

Manuel Hermenegildo:

8. Steering Committee of the Static Analysis Symposium (SAS).

9. Steering Committee of the International Symposium on Functional and Logic Programming (FLOPS).

10. Steering Committee of the International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI).

11. Editorial Advisor and former Area Editor (architecture and implementation) of "Theory and Practice of Logic Programming" (Cambridge U. Press)

12. Associate Editor of the "Journal of New Generation Computing" (Springer-Verlag)

13. Area Editor of "Journal of Applied Logic" (Elsevier North-Holland).

14. Board of the new IGPL Journal of Algorithms in Cognition, Informatics and Logic.

Juan José Moreno:

15. Editorial Board member GSTF Journal on Operating Systems and Programming Languages (JOSPL).

6.3.4. Association and Organization Committees

Gilles Barthe:

1. Organizing committee of the International School on Foundations of Security Analysis and Design.

2. Dagsthul seminar on The synergy between programming languages and cryptography.

Manuel Carro:

3. Manager, EIT ICT Labs Co-Location Center Madrid, and R&D Co-ordinator.

4. ALP Summer school on computational logic, 2014.

Carolina Dania:

5. Co-organizer of the 14th International Workshop on OCL and Textual Modeling Applications and Case Studies (OCL 2014).

Dario Fiore:

6. Vice-chair of COST Action IC1306 "Cryptography for Secure Digital Interaction."

7. Organization committee of the COST School on Cryptographic Attacks, Porto, October 2014.

Alessandra Gorla:

8. Co-organizer of the GI-Dagstuhl Seminar on Software Engineering for Self-Adaptive Systems, October 2014.

Alexey Gotsman:

9. Workshop on Principles and Practice of Eventual Consistency, affiliated with EuroSys (PaPEC 2014).

Manuel Hermenegildo:

10. Director, EIT ICT Labs Madrid Associate Partner Group.

11. Elected member Informatics Europe steering board.

12. Elected President of SpaRCIM.

13. Member *Academia Europaea*.

14. Member Dagstuhl scientific advisory board.

15. Member IRILL (French Free Software Institute) scientific board.

16. Member Informatics Europe department evaluation board.

17. Member IFCoLog advisory board.

Dragan Ivanovic:

18. Project and Marketing & Communication Officer, EIT ICT Labs Madrid Associate Partner Group.

Juan José Moreno:

19. Chair of the Spanish Scientific Society for Software Engineering and Development Technologies.

20. Deputy Director, EIT ICT Labs Madrid Associate Partner Group.

21. Jury member of the Innovative Companies Forum 2014.

22. Jury member of the National Awards Computer Science 2014.

23. Jury member of Desafío Educacíon - Telefonica 2014.

Pavithra Prabhakar:

24. Co-organizer of the Dagstuhl seminar on Verification of Cyber-Physical Systems, March 2014.

Pierre-Yves Strub:

25. Co-organizer of the Joint EasyCrypt-F*-CryptoVerif School, Paris, November 2014.

6.4. Awards

1. *Juan José Moreno*: Sociedad Espanola de Ingeniería de Software y Tecnologías de Desarrollo de Software (SISTEDES) Award 2014.

awards

$R_{rng}^{[k]} = R_{all}$

$\wedge\ R_{all} = R_{rng}^{[k]} \cup \bigcup_{j \in 1..3} R_j^{[k]} \quad \wedge \quad \bigcup_{j \in T_{ID} - \{k\}} R_3^{[j]}$

$\cup\ R_3^{[k]} \quad \wedge\ R_3^{[k]} \# R_{rng}^{[k]} \quad (\wedge\ Graph(root$

Inv Inv

$r) \wedge n \in r \rightarrow Graph(n, r') \wedge r' \subseteq r$ lo v. (Lemm

$, r) \longrightarrow \bigcup_{i \in 1..3} R_i^{[k]} \subseteq r$ (Construc. + Hex Pred)

$= R_2^{[k]} = emp$ (Teo)

Si $n \in R_3^{[k]}$, listo.

$Inv^{[k]}$ Sabemos q' $n \in r \rightarrow n \in \bigcup_{j \in 1..3} R_j^{[k]} \vee n \in$

Nad

$n \in R_1^{[k]} \cup R_2^{[k]}$. Luego $n \in stk^{[k]}$ (por 3)

e remueve de $stk^{[k]}$ solo si $n \in R_3^{[k]}$

nos, at_end $\rightarrow stk^{[k]} = empty$ $\therefore$ at_end $\rightarrow R_1^{[k]} \cup R_2^{[k]}$

$^{[k]}$ $\rightarrow n \in stk^{[k]}$ (Construc

scientific highlights

7.1. Computer-Aided Cryptographic Proofs [94]

7.2. Energy Transparency for Developing Energy-Efficient Software [96]

7.3. Architecture-Driven Verification of Systems Software [98]

7.4. Formal Verification of Stability of Embedded Control Systems [100]

7.5. Cyber-Attack Detection from Network Traffic [102]

annual report 2014

computer-aided cr

Computer-Aided Cryptographic Proofs

To deal with the rising complexity of cryptographic proofs, researchers from the IMDEA Software Institute and INRIA are developing EasyCrypt, an SMT-based tool for writing and checking cryptographic security proofs. The tool has been used to build machine-checked proofs of widely deployed cryptographic algorithms and protocols. Recent achievements include a formally verified x86 implementation of the PKCS#1 standard (using EasyCrypt in combination with the CompCert verified compiler) [1], and a modular proof of security for one-round key exchange protocols such as Naxos [2]. Externally, EasyCrypt is used by the Microsoft Research-INRIA joint centre in the context of the MiTLS project, and at the MIT Lincoln Laboratory. A first summer school and workshop dedicated to EasyCrypt took place at the University of Pennsylvania in July 2013, gathering more than 30 participants. A second summer school dedicated to EasyCrypt, CryptoVerif and F* took place in Paris in November 2014, attracting more than 70 participants.

The team is exploring two main directions of research: automated analysis of cryptographic constructions and applications to real-world cryptographic systems. The first line of work is funded by the US Office of Naval Research (ONR). The project, which involves the IMDEA Software Institute, Stanford University, University of Pennsylvania and SRI, has made significant progress. In collaboration with colleagues at INRIA, researchers at the IMDEA Software Institute have developed automated methods, inspired from program synthesis, to perform an exhaustive analysis of encryption schemes based on RSA [3]. These methods, implemented in ZooCrypt, have led to the discovery of a new and efficient scheme, called ZAEP [4]. Moreover, they have also applied synthesis techniques to discover new fault attacks on elliptic curve implementations [5]; such attacks are particularly effective in the setting of embedded systems, where adversaries can tamper with the execution of cryptographic algorithms, using for instance laser beams to reset a register to a default value. In collaboration with researchers at University of Pennsylvania and Stanford, researchers at the IMDEA Software Institute have also developed an automated tool for analyzing the validity of hardness assumptions in the generic group model [6]. This tool can be used by cryptographers, without any previous knowledge of

yptographic proofs

formal methods, to ensure that the hardness assumptions that they use to justify their constructions are not vulnerable to algebraic attacks.

Related publications

[1] J.B. Almeida, M. Barbosa, G. Barthe and F. Dupressoir, "Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations," in 20th ACM Conference on Computer and Communications Security, CCS 2013.

[2] G. Barthe, J.M. Crespo, Y. Lakhnech, and B. Schmidt, "Mind the Gap: Modular Machine-checked Proofs of One-Round Key Exchange Protocols" in 34th European Conference on Advances in Cryptology, Eurocrypt 2015.

[3] G. Barthe, J. Crespo, B. Grégoire, C. Kunz, Y. Lakhnech, B. Schmidt and S. Zanella-Béguelin, "Fully automated analysis of padding-based encryption in the computational model," in 20th ACM conference on computer and communications security, CCS 2013. 2013, pp. 1247–1260.

[4] G. Barthe, D. Pointcheval and S. Zanella-Béguelin, "Verified security of redundancy-free encryption from Rabin and RSA," in 19th ACM conference on computer and communications security, CCS 2012. 2012, pp. 724–735.

[5] G. Barthe, F. Dupressoir, P. Fouque, B. Grégoire and J. Zapalowicz, "Synthesis of fault attacks on cryptographic implementations," in 21th ACM Conference on Computer and Communications Security, CCS 2014.

[6] G. Barthe, E. Fagerholm, D. Fiore, J. C. Mitchell, A. Scedrov and B. Schmidt, "Automated analysis of cryptographic assumptions in generic group models," in 34th Conference on Advances in cryptology, Crypto 2014.

energy tran

for developing energy-efficient software

Energy Transparency for Developing Energy-Efficient Software

An important part of the IMDEA Software Institute's research on energy-efficient software development is performed in the context of the EU FP7 FET project "ENTRA: Whole-Systems Energy Transparency," in collaboration with Roskilde University (Denmark), the University of Bristol (UK) and XMOS Ltd (UK) (described in Chapter 5).

Achieving *energy transparency* through the system layers, from machine code to source code, implies that energy consumption at the hardware layer should be immediately visible at the layer at which software is designed or used.

The results so far include techniques and tools that enable energy transparency, such as a multi-level static program analysis [2,3,4,8] that estimates the energy consumed by programs as functions on input data size obtained at compile-time (using abstract interpretation), i.e., without actually running the programs. The analysis uses low-level models of machine instructions and infers energy consumption at different levels, including assembly and the compiler intermediate representation (LLVM IR), as well as upwards reflection to the source-code level. In addition, other techniques and tools based on the energy transparency view have been developed, such as a system for the verification of energy consumption specifications [5], and program optimization techniques [1] that exploit useful features offered by current hardware (such as Dynamic Voltage and Frequency Scaling–DVFS) together with task scheduling techniques for multi-core systems.

Current work focuses on extending and consolidating the results so far, especially the optimization techniques, maturing the prototype tools for analysis, verification and optimization, in order to enable engineers to understand and quantify the impact of design decisions on energy, and coming up with a set of recommendations for the integration of such energy-aware tools in the software life-cycle.

sparency

Related publications

[1] Z. Banković and P. Lopez-Garcia. Stochastic vs. Deterministic Evolutionary Algorithm-based Allocation and Scheduling for XMOS Chips. *Neurocomputing*, 150(0):82–89, February 2015. To Appear.

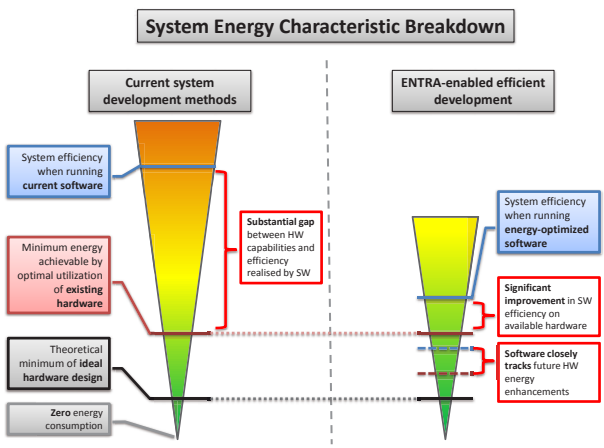
[2] K. Georgiou, U. Liqat, P. Lopez-Garcia, M.V. Hermenegildo, and K. Eder. Towards LLVM-Based Energy Consumption Analysis of Programs. ICT-Energy (Nanoenergy) Letters (8), July 2014.

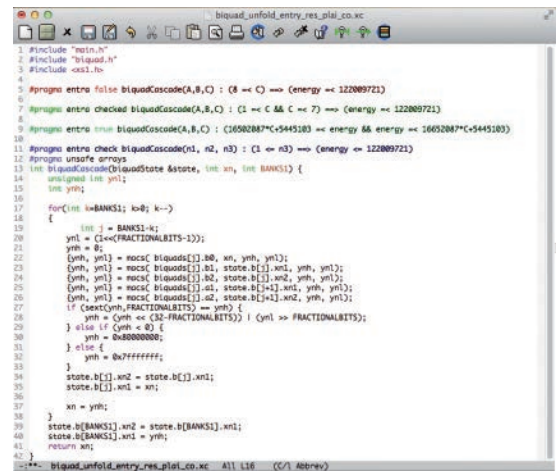
[3] U. Liqat, S. Kerrison, A. Serrano, K. Georgiou, P. Lopez-Garcia, N. Grech, M.V. Hermenegildo, and K. Eder. Energy Consumption Analysis of Programs based on XMOS ISA-level Models. In *Proceedings of the 23rd International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'13)*, 2014.

[4] U. Liqat, K. Georgiou, S. Kerrison, P. Lopez-Garcia, M.V. Hermenegildo, J.P. Gallagher and K. Eder. Inferring Energy Consumption at Different Software Levels: ISA vs. LLVM IR. Deliverable D3.2, ENTRA Project, Appendix D3.2.4 (http://entraproject.eu).

[5] P. Lopez-Garcia, R. Haemmerlé, M. Klemen, U. Liqat, and M. V. Hermenegildo. Towards Energy Consumption Verification via Static Analysis. In *Workshop on High Performance Energy Efficient Embedded Systems (HIP3ES 2015)*, 2015. To Appear.

[6] A. Serrano, P. Lopez-Garcia, and M. Hermenegildo. Resource Usage Analysis of Logic Programs via Abstract Interpretation Using Sized Types. *Theory and Practice of Logic Programming, 30th Int'l. Conference on Logic Programming (ICLP'14) Special Issue*, 14(4-5):739–754, 2014.





architecture-dri

Architecture-Driven Verification of Systems Software

of systems software

The research in architecture-driven verification of system software at the IMDEA Software Institute is performed in part within the scope of the EU project ADVENT, an FP7 FET Young Explorers project started in 2013 and coordinated by IMDEA Software in cooperation with Katholieke Universiteit Leuven (Belgium), Max Planck Institute for Software Systems (Germany) and Tel-Aviv University (Israel). The research is also supported by a Microsoft Software Engineering Innovation Foundation Award and a Microsoft European PhD Scholarship.

The key element of the ADVENT approach is to base the design of advanced verification techniques on formalization of software engineering concepts already used by systems programmers to reason about their software informally. By taking advantage of programmers' knowledge and intuition, this approach improves on the common practice of building generic verification tools that fail to scale to big and complicated systems.

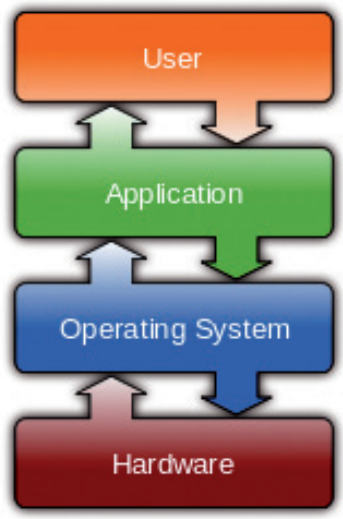
The architecture-driven techniques have the potential to result in verification tools that require a minimal and intuitive user input — essentially equivalent to a formal version of the high-level informal specifications programmers already have in mind when developing software. In time, this can yield a dramatic leap in the cost-benefit ratio of the verification technology, allowing it to scale to systems of real-world size and complexity that have so far been beyond the reach of quality assurance methods for guaranteeing correctness.

ven verification

Related publications

[1] Hagit Attiya, *Alexey Gotsman*, Sandeep Hans, Noam Rinetzky. A Programming Language Perspective on Transactional Memory Consistency. Proceedings of the 32nd ACM Symposium on Principles of Distributed Computing (PODC'13), Montreal, Canada, pages 309–318, ACM Press, 2013.

[2] Sebastian Burckhardt, *Alexey Gotsman*, Hongseok Yang, Marek Zawirski: Replicated data types: specification, verification, optimality. Proceedings of POPL 2014. ACM Press, 2014.



formal verificat

Formal Verification of Stability of Embedded Control Systems

of embedded control systems

Stability is a base requirement in the design of embedded control systems. The stability of a control system is often extremely important and is generally a safety issue in the engineering of a system. As stated by Gunter Stein, chief scientist at Honeywell technology in the first Hendrik W. Bode lecture, "Unstable systems are fundamentally and quantifiably more difficult to control than stable ones. Controllers for unstable systems are operationally stable." In fact, there have been instances where the presence of unstable components have had catastrophic consequences. The Gripen JAS-39 prototype airplane which consisted of unstable elements crash landed in 1989 in one of its first test flights. The most formidable of all is the Chernobyl nuclear reactor disaster, which left hundreds of people dead and incurred millions of dollars in clean-up cost.

The researchers at IMDEA are developing a novel methodology and software tools for scalable verification of stability by borrowing insights from formal methods, control theory and dynamical systems theory. In particular, the goal is to develop an algorithmic framework accompanied by abstraction-refinement techniques which will perform a systematic exploration of the abstraction space to find a proof of stability. This is in contrast to existing deductive techniques which try to find functions with certain properties (for instance, Lyapunov functions) that act as certificates of stability. Here, a template is fixed for a candidate Lyapunov function, and the parameters of the template are found by solving certain constraint solving problems. These methods suffer from numerical instability. More importantly, their success depends on the right choice of templates which requires user ingenuity. To summarize, our approach promises a fully automated framework and has negligible numerical instability issues.

This work is being conducted as part of the VeriStab project which is supported by a Marie Curie Career Integration Grant from the EU FP7 program. The project is being lead by Prof. Pavithra Prabhakar and is supported by her group. One of the foundational papers on this project has received an honorable mention best paper award [7], and

ion of stability

two of the papers [2, 6] have been invited for presentation at the conferences. A tool AVERIST (Algorithmic VERIfier for Stability) is under development as part of the project.

Related publications

[1] P. Prabhakar and M. Garcia Soto. Foundations of Quantitative Predicate Abstraction for Stability Analysis of Hybrid Systems. *Verification, Model-Checking and Abstract Interpretation* (VMCAI), 2015.

[2] P. Prabhakar and M. García Soto. An algorithmic approach to stability verification of polyhedral switched systems. *Americal Control Conference* (ACC), 2014.

[3] P. Prabhakar and M. García Soto. Abstraction Based Model-Checking of Stability of Hybrid Systems. *25th International Conference on Computer Aided Verification* (CAV), 2013.

[4] P. Prabhakar, J. Liu and R. M. Murray. Pre-orders for reasoning about stability properties with respect to input of hybrid systems. *International Conference on Embedded Software* (EMSOFT), 2013.

[5] P. Prabhakar and M. Viswanathan. On the decidability of stability of hybrid systems. *16th international conference on Hybrid systems: computation and control* (HSCC), 2013.

[6] P. Prabhakar. Foundations for approximation based analysis of stability properties of hybrid systems. *50th Annual Allerton Conference on Communication, Control, and Computing* (Allerton), 2012.

[7] P. Prabhakar, G. E. Dullerud and M. Viswanathan. Pre-orders for reasoning about stability. *Hybrid Systems: Computation and Control* (HSCC), 2012.

cyber-attack

Cyber-Attack Detection from Network Traffic

from network traffic

CADENCE (Cyber Attack Detector ENgineering for Commercial Exploitation) is a security sensor capable of detecting cyberattacks in network traffic by applying novel anomaly detection techniques. CADENCE is a project funded by the European Institute of Technology (EIT) ICT Labs during 2014 and 2015. The CADENCE consortium comprises 3 European partners: TNO (The Netherlands), Reply Communications Valley (taly), and the IMDEA Software Institute.

The goal of the CADENCE project is to develop and commercialize the CADENCE sensor, which monitors network traffic in an enterprise network and detects Advanced Persistent Threats (APTs) and malware communication with its remote infrastructures. The project focuses on innovation with the goal of maturing previous technologies developed by the partners and converting them into a product.

During 2014 the first CADENCE sensor prototype was developed based on key technologies from the partners, and an initial business plan and market analysis were prepared. For 2015, the development of the current sensor prototype continues with an emphasis on mobile devices that may be present on the enterprise network. The overarching goal

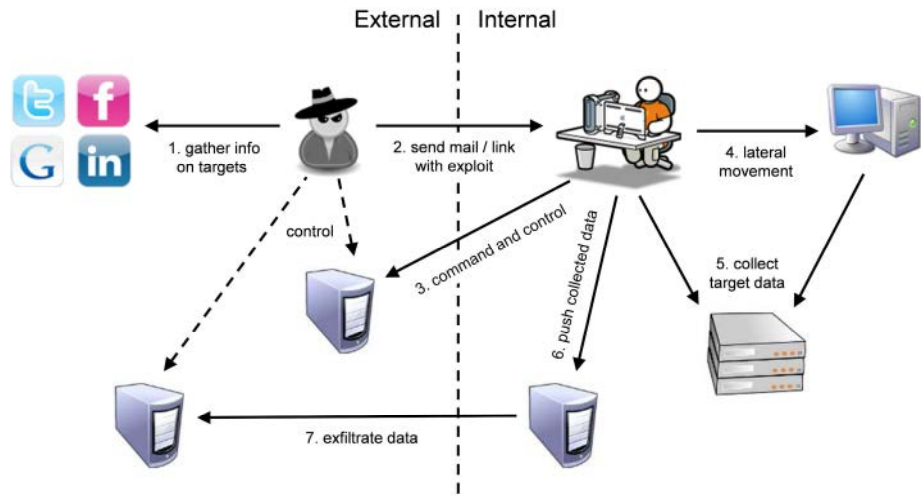
for 2015 is to launch a startup that commercializes the CADENCE sensor. The startup will be based at the incubator node of EIT ICT Labs in Trento, Italy.

Recently, the CADENCE project has been awarded an honourable mention for public-private cooperation leading to commercialization of research results at the 10th Madri+d awards.

Related publications

[1] M. Zubair Rafique and Juan Caballero. "FIRMA: Malware Clustering and Network Signature Generation with Mixed Network Behaviors". In Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses, St. Lucia, October, 2013.

[2] Antonio Nappa, M. Zubair Rafique, and Juan Caballero. "Driving in the Cloud: An Analysis of Drive-by Download Operations and Abuse Reporting". In Proceedings of the 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Berlin, Germany, July 2013.



editor
imdea software institute

graphic design
base 12 diseño y comunicación

photos on pages 12 and 13
Daniel Schäfer

photo in cover
Víctor Castelo

legal deposit number
M-9.009-2015

La Suma de Todos
Comunidad de Madrid
www.madrid.org

EUROPEAN UNION
STRUCTURAL FUNDS

www.software.imdea.org

institute IMDEA software

Contact
software@imdea.org
tel. +34 91 101 22 02
fax +34 91 101 13 58

Instituto IMDEA Software
Campus de Montegancedo
28223 Pozuelo de Alarcón
Madrid, Spain

annual report

2014