imdea software institute

science and technology for developing better software

institute imdea software

annual report 2015

imdea software institute

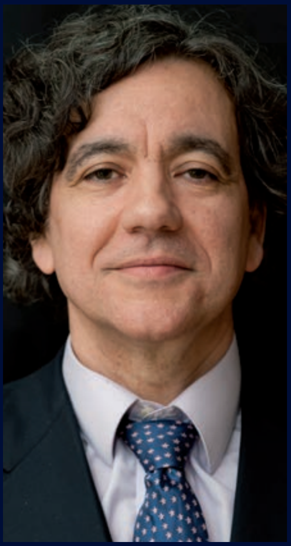
science and technology for developing better software

institute imdea software

annual report

2015

foreword



Manuel Hermenegildo
Director, IMDEA Software Institute
April 6, 2016

The IMDEA Software Institute was created by the Madrid Regional Government under the strong belief that quality research and innovation in technology-related areas is the most successful and cost-effective way of generating knowledge, competitiveness, sustainable growth, and employment. This is more relevant in current times 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, that has reached world-class status in its objectives of excellence in attraction of talent, 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 23 faculty (one half-time), 10 postdocs, 4 senior visitors, 26 research assistants, 12 project staff, a number of interns, and 8 staff members, from 17 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 150 international researchers have visited and given talks at the Institute to date.

During 2015 Institute researchers have published 81 refereed publications (in some of the top venues in the field, such as POPL, CRYPTO, EUROCRYPT, IEEE S&P, ACM CCS, CSF, CAV, ICLP, ICALP, etc.), given 21 invited talks and 43 invited seminars and lectures, and participated in 65 program committees and 21 boards of journals and conferences, in addition to being conference or program chairs of 6 conferences. The Institute has received 13 best paper awards or mentions in the last 5 years.

The Institute has also participated during 2015 in 30 funded research projects and contracts and received 9 fellowships. 19 of the projects are from international agencies (16 funded by the EU, 3 by the US agencies ONR and NIST), 5 are direct industrial funding, and 77% of them (23) involve collaboration with a large number of companies of all sizes, about 50% Spanish and the rest from other EU countries and the US. These include Atos, Siemens, Deimos, AbsInt, Microsoft, Fredhopper, Telefónica, Boeing, Thales, Scytl, 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 Cadence and ActionGUI technologies, with ETH Zurich, TNO, and Reply.

In 2015 the Institute has also strengthened further its strategic partnership with Telefónica, Indra, Atos, UPM, and BSC, including a significant increase of the activities of the European Institute of Innovation and Technology community EIT Digital KIC 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, entrepreneurship, and business development, including coaching and hosting several startups. The Institute has also continued its strong collaborations with Microsoft, within the Microsoft Research–IMDEA Software Joint Research Center, and with Telefónica through our Joint Research Unit. In the context of all these activities, during 2015 the Institute has hosted a good number of events centered around innovation and entrepreneurship.

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

table of contents

table of contents

annual report

2015

general presentation

1

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 attraction of talent, research of excellence, and technology transfer in 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.

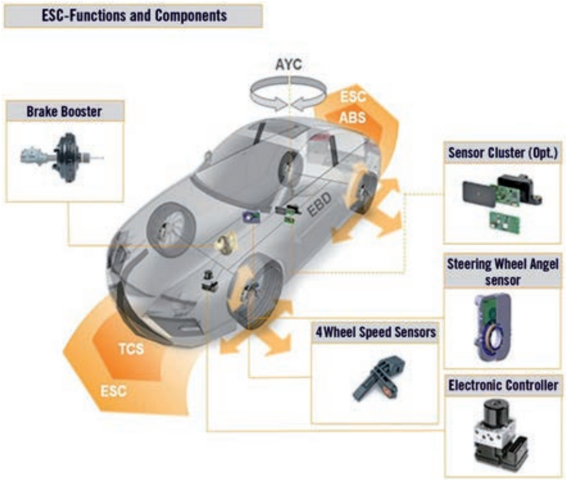
The IMDEA Software Institute is part of the Madrid Institutes for Advanced Studies (IMDEA), an institutional framework created to foster social and economic growth in the region of Madrid by promoting research of excellence and technology transfer in a number of strategic areas (water, food, energy, 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 in third quarter of 2015, global IT spending in 2016 is expected to grow by 1.7% and exceed 3.5 trillion USD, with the annual growth rate close to 2.7% for the 2017-19 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, it is not surprising that errors, failures and vulnerabilities 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 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 U.S. economy at $60 billion annually, or about 0.6 percent of GDP. The reason for this high cost is that,



Modern cars and trucks contain as many as 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.

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.

The security of software systems is also paramount. The European Commission estimates that the damage costs due to cyber-attacks in the European Union is in the order of billions each year. In 2013 a single data breach costed a US retail company $160 million, more than a 40% drop in its profits. Developing software technologies that can detect malicious behaviors and provide defense mechanisms against cyber-attacks is therefore of primary importance.

However, producing automatic tools for reducing software errors as well as developing detection and defense technologies against cyberattacks is extremely hard, 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, safety, 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 world-wide, 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 and innovation.

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.

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.

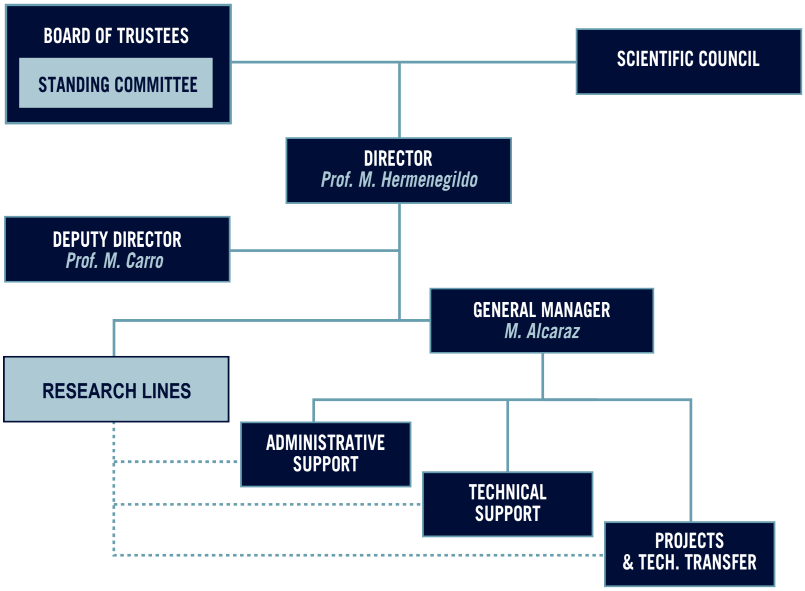


Figure 1.1. Governance and management structure of the IMDEA Software Institute.

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

Ms. Alicia Delibes Liniers, Vice-Councilor for Education, Youth, and Sports and Vice-President of the Board of Trustees, left her position in the Regional Government during 2015 and was replaced by Mr. Rafael van Grieken Salvador, Councilor for Education, Youth, and Sports, who was appointed Vice-President of the Board of Trustees. Ms. Lorena Heras Sedano was replaced as Director General for Universities and Research by Mr. José M. Torralba Castelló, who was appointed member of the Board. Mr. Juan A. Botas Echevarría, Deputy Director-General for Universities and Research was replaced in his position and in the Board by Mr. Rafael García Muñoz. Finally, Mr. José M. Rotellar García, former Vice-Councilor for Finance and Economic Policy, left his position in the Regional Government and also in the Board of Trustees.

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

Ilmo. Sr. D. Rafael van Grieken Salvador
Councilor for Education, Youth and Sports, Madrid Regional Government, Spain.

MADRID REGIONAL GOVERNMENT

Ilmo. Sr. D. Rafael van Grieken Salvador
Councilor for Education, Youth and Sports, Madrid Regional Government, Spain.

Ilmo. Sr. D. José Manuel Torralba Castelló
Director-General for Universities and Research, Madrid Regional Government, Spain.

Ilmo. Sr. D. Rafael García Muñoz
Deputy Director-General for Research, Madrid Regional Government, Spain.

UNIVERSITIES AND PUBLIC RESEARCH BODIES

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

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

Prof. Víctor Robles Forcada
Universidad Politécnica de Madrid, 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, and Estanislao Fernández González-Colaço.

Elecnor Deimos
Mr. Miguel Belló Mora, General Director (later moved to UrtheCast), Mr. Carlos Fernández de la Peña, Director of Business Development, and Mr. Felipe Bertrand, Project Manager.

Atos
Mr. José María Cavanillas, Chief Big Data & Security Officer, and Ms. Clara Pezuela, Head of IT Market.

Indra
Mr. Juan L. Martín Ruiz, Director for Innovation Management.

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. These premises offer an ideal environment for fulfilling its mission of attraction of talent, 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 EIT Digital KIC, part of the European Institute of Innovation and Technology, the IMDEA Software-Microsoft Joint Research Center, the IMDEA Software-Telefónica 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 Science and Technology Park. These centers include the Madrid Center for Supercomputing and Visualization (CESVIMA), the Center for Computational Simulation, 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 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

annual report 2015

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.

Collaborative Projects and Contracts. 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.

Strategic Partnerships. The Institute has 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 Telefónica, Indra, Atos, and BBVA which have led to a number of strategic cooperation initiatives. An important instance of these initiatives is the joint establishment of the Spanish Associate Partner Group of EIT Digital, the ICT branch of the European Institute of Innovation and Technology, with the added participation of UPM and BSC, and coordinated by the Institute. The coordination of EIT Digital Madrid includes the hosting and operation of the EIT Digital Madrid Co-Location Center and many other joint activities in training (at Masters and PhD level), innovation, and entrepreneurship. In addition, the Institute has established with Telefónica the *Telefónica-IMDEA Software Joint Research Unit* and with Microsoft the *Microsoft Research–IMDEA Software Joint Research Center*, and is planning the creation of more such units with other industrial partners. These activities are later described in more detail.

The 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.

Commercialization of Technology. Another important form of technology transfer is the *commercialization of the 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,

CLUSTER
Madrid Network

eit
Digital

es.INTERNET

together with the licensing of such technology (e.g., the CADENCE technologies have been licensed to Reply Communication Valley, see Chapter 7), 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 also under way); GGA; EasyCrypt, ZooCrypt, and Masking (the latter three developed jointly by IMDEA Software and INRIA).

Other Industrial Funding and Collaborations. 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.

Atos
BBVA
BOEING
Bull
EADS astrium
france telecom
Microsoft Research
SAP
gtd
AbsInt Angewandte Informatik
AIRBUS
lambdastream
DAIMLER
deimos space
flexiant utility computing on demand
Fredhopper®
iberia
Institut für Bahntechnik GmbH Berlin · Dresden
INTEGRASYS
Nokia Siemens Networks
PSA PEUGEOT CITROËN
SIEMENS
2ndQuadrant Professional PostgreSQL
THALES
tecnalia Inspiring Business
Telefónica Investigación y Desarrollo
TELECOM ITALIA
treelogic enjoy the change
Trusted Labs
XMOS®
orange™
ENGINEERING
LogicBlox
Reply Living network
zemsania Tech Services & Solutions
Scytl Innovating Democracy
Indra

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	Telefónica	Telefónica I+D
Contracts	LogicBlox	LogicBlox
Contracts (eTUR2020)	Zemsannia	Zemsania, Tecnocom, Groupalia, Solusoft, Eurona, BDigital

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

2.2. Cooperation with Research Institutions

As an 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. Furthermore, all of the seminars and talks at the Institute are open to the campus and the academic community at large.

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 has been collaborating with UPM in a graduate program for several years. This program is instrumented as a separate track on *Software Development through Rigorous Methods* in an existing Masters ("MUSS") and PhD programs ("DSS / DSSC") at UPM. In them, researchers from the Institute can teach through a "Venia Docendi", i.e., a permission to teach, and be PhD thesis advisors. Most research assistants at the IMDEA Software Institute obtain their Masters and PhD following these programs. Under the agreement with the Consejo Superior de Investigaciones Científicas, two researchers—Cesar Sánchez and Pedro López—have dual appointments at CSIC and 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 Institute 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 institutes, 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 Digital

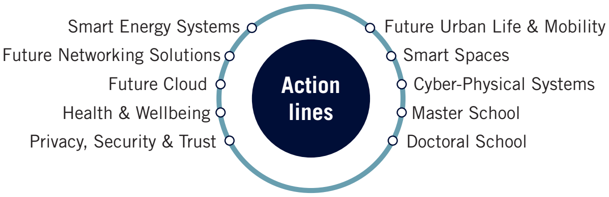
In June 2013, IMDEA Software officially became an Associate Partner of EIT Digital (formerly known as EIT ICT Labs), as the first Spanish organization to enter its Pan-European network of seven full national nodes (in Helsinki, Stockholm, Berlin, London, Eindhoven, Paris, and Trento) and two associate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

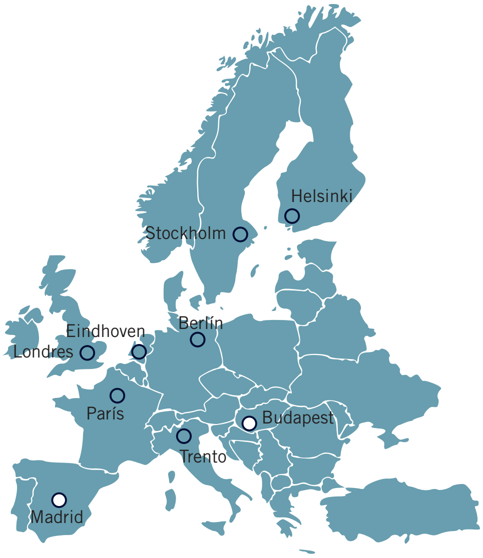
EIT Digital is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT), which includes some of the leading educational, research, and industrial actors in the ICT innovation ecosystem in Europe. Its mission is to combine the educational, research, and 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 integrated and innovation-driven Master and Doctoral Schools and Business Development Acceleration programs.

One of the key goals of IMDEA Software as the Spanish Associate Member is to promote, motivate, and organize the presence of EIT Digital 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, and the Technical University of Madrid (UPM) – towards a fully operational EIT Digital node. Together with these strategic partners, the Institute is working on developing innovation-oriented projects within the framework of EIT Digital, 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 Digital Business Plan for 2015 with the following activities:

- Research and innovation activity in the field of Privacy, Security, and Trust (project CADENCE, continuing from 2014 – see Chapter 5 for more details).
- Further development of the Madrid Co-Location Center (CLC), hosted in the premises of IMDEA Software. The CLC is the home for the EIT Digital activities and the meetings of the Spanish APG, and has the objective of fostering innovation, technology transfer, and entrepreneurship in Spain. The CLC is equipped with ample office space and meeting facilities, workspaces for start-ups, and work and collaboration areas for the students in the EIT Digital masters and doctoral programs. In addition to the organization and participation in relevant events devoted to innovation (e.g., the South Summit), the CLC also hosts startups and scaleups. During 2015 three companies, participating in the EIT Digital Accelerator Program, have been coached and hosted at the CLC: Coowry, LeanXcale, and LocaliData.





- Development of the Madrid Business Development Accelerator (BDA) segment which is part of the EIT Digital BDA 50-strong specialists network who help 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., the South Summit.

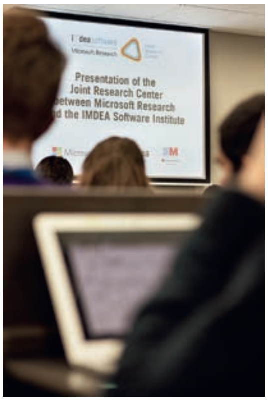
- Launch of the EIT Digital Doctoral Training Center and the Master Program in Data Analytics, in cooperation with UPM, which is part of the EIT Digital educational initiative that allows doctoral and master students to obtain not only a recognized technical education, but also entrepreneurial skills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

2.4. Microsoft Research - IMDEA Software Joint Research Center

Joint Research Center
institute IMdea software
Microsoft Research

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 second Microsoft Research - IMDEA Software Institute Collaborative Workshop (MICW 2015) took place at the IMDEA Software Institute on April 9-10, 2015. This was the second in a series of annual workshops aimed at reinforcing the collaboration between the two institutions, with researchers from both sides working together on several research topics. It was organized by Judith Bishop and Cedric Fournet from Microsoft Research and by Alexey Gotsman and Manuel Hermenegildo from the IMDEA Software Institute.


Presentation of the Joint Research Center between Microsoft Research and the IMDEA Software Institute

The collaborative workshops bring together researchers and students to discuss their joint work on hot topics in software in order to advance the state of the art and, where possible, to bring those advances to market. The second workshop included sessions on Scalable and Correct Data Management in the Cloud, Verification for Cryptography and Security, and Secure Distributed Programming, as well as ample time for focussed group discussions.

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 joint papers at top-ranked conferences such as ACM Symposium on Principles of Programming Languages (POPL), IEEE Symposium on Security and Privacy (S&P), and International Conference on Computer Aided Verification (CAV).

2.5. Telefónica - IMDEA Software Joint Research Unit

IMDEA Software and Telefónica I+D cooperate since 2012 on developing software architectures and high-level components within the framework of the FI-WARE initiative through a Joint Research Unit. This 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. The Joint Research Unit also organizes education activities in the area of FI-WARE technology.

Telefónica Investigación y Desarrollo

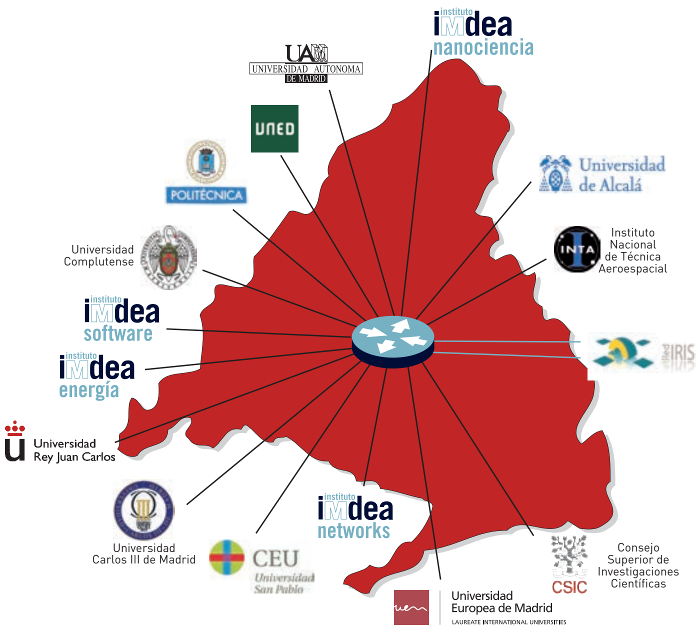
2.6. REDIMadrid

REDIMadrid

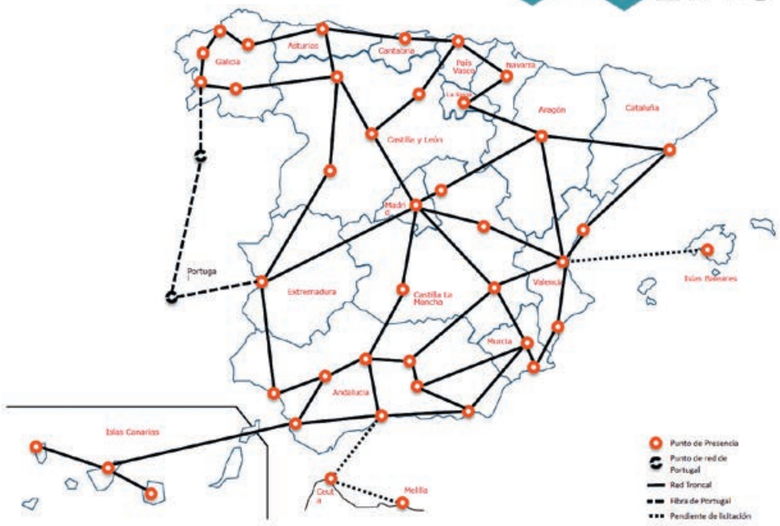
REDIMadrid is the academic and research Internet backbone of the Madrid Region, which connects universities and research centers located in the Madrid region (including IMDEA Software and the other IMDEA institutes). REDIMadrid is currently managed by the IMDEA Software Institute, and it is funded by the Madrid Regional Government. REDIMadrid provides the connected institutions with a highly-reliable high-speed connection to the REDIMadrid routing facilities, which connects to the national network (RedIRIS), the European research network Géant and the rest of the Internet. For example, all public universities are provided connections at 10Gb per second using a network of metropolitan fiber-optic rings.

The IMDEA Software Institute also hosts and operates the new *EIT Digital node*, located at the data center of the EIT Digital Co-location Center. This node is connected to the REDIMadrid infrastructure using a fiber-optic link provided by the National High-Speed Research Network Backbone, *RedIRIS-NOVA*. This pioneer link is operated as an experimentation infrastructure that supports speeds of up to 100Gb, and whose routing facilities have been designed, deployed and maintained by the IMDEA Software REDIMadrid personnel. This recent expansion of RedIRIS-NOVA and REDIMadrid has been funded jointly by the Spanish and Madrid Governments in direct support of the EIT Digital associate partner group in Spain.

REDIMadrid


instituto imdea nanociencia
UAM Universidad Autónoma de Madrid
UNED
Politécnica
Universidad de Alcalá
Universidad Complutense
INTA Instituto Nacional de Técnica Aeroespacial
instituto imdea software
RedIRIS
instituto imdea energía
Universidad Rey Juan Carlos
instituto imdea networks
Universidad Carlos III de Madrid
CEU Universidad San Pablo
CSIC Consejo Superior de Investigaciones Científicas
uem Universidad Europea de Madrid LAUREATE INTERNATIONAL UNIVERSITIES

NOVA RedIRIS



research

3

annual report

2015

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. We pursue our mission by focusing on three strategic areas, namely *Program Analysis and Verification*, *Languages and Compilers*, and *Security and Privacy*:

- Our research on *Program Analysis and Verification* advances the foundations and the tools that enable software engineers understand the key properties of the complex systems they are building. Our results range from tools that automatically establish proofs of correctness and safety, which is paramount, for example, for avionics software, to tools that explore energy consumption profiles at design time, which is fundamental for mobile and embedded devices.

- Our research on *Languages and Compilers* provides software engineers with the means they need to describe their ideas in more concise and modular ways, and to generate correct and performant executables from these descriptions. Progress in this area has the potential to dramatically increase programmer productivity as well as maintainability and reusability of software.

- Our research on *Security and Privacy* delivers technology that enables computation, communication, and storage in untrusted and malicious enviroments, such as the Internet. Our results include novel cryptographic protocols as well as cutting-edge techniques for detecting and analyzing malicious activities and vulnerabilities in software, hardware, and network traffic.

The remainder of the chapter describes in more detail the key lines of research that are currently pursued by the scientists of IMDEA Software.

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, sensors, and portable/implantable medical devices. 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. Energy consumption is also highly relevant in the context of the *Internet of Things* paradigm, where very large numbers of small autonomous devices (expected to reach about 50 *billion* by the year 2020), embedded in all kind of objects, in our clothes, or stuck to our bodies, will operate and intercommunicate continuously for long periods of time, such as years. Although there have been improvements in battery and energy harvesting technology, a significant reduction in the energy demands of such devices is needed to make the full *Internet of Things* vision come true and all its potential be exploited.

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 have promoted energy efficiency to a first-class goal in software design, and developed techniques and 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).

These state-of-the-art techniques and tools are implemented and integrated into the pioneering CiaoPP system, which provides a general, sound, and practical framework (based on abstract interpretation) for predicting with high accuracy the resources consumed by a given piece of software, for debugging/certifying such consumption with respect to specifications, and for generating dynamic optimization strategies. The system 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

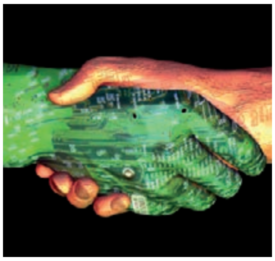
execution time, resulting in significant improvements in battery life (e.g., in smart phones and other small devices), or reductions in electricity consumption (e.g., at data centers).

In close collaboration with industry, IMDEA's energy-aware tools are integrated into their products, and tested on concrete industrial applications. 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 those of the United States and the European Union, have established several funding initiatives to exploit this potential. Cyber-physical systems invariably appear 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.



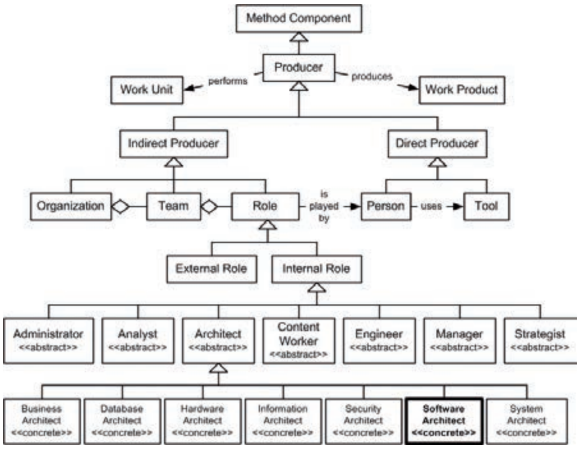
While formal methods have been successfully applied to the analysis of stand-alone hardware and software, CPS differ from traditional software in the tight interactions with the physical system it controls, and in that CPS run on one or more embedded processors which communicate with each other. Hence, 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.

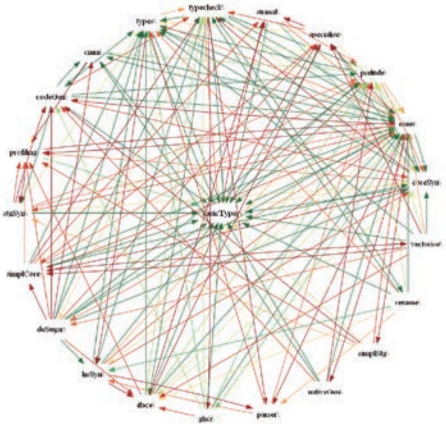
Researchers at the IMDEA Software Institute are actively involved in this exciting new area by focusing on the development of the state-of-the-art technology for verification of cyber-physical systems, particularly, in the early design phase, where reliability has a huge impact on the development cost 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.


Method Component
Producer
Work Unit
performs
produces
Work Product
Indirect Producer
Direct Producer
Organization
Team
Role
is played by
Person
uses
Tool
External Role
Internal Role
Administrator <<abstract>>
Analyst <<abstract>>
Architect <<abstract>>
Content Worker <<abstract>>
Engineer <<abstract>>
Manager <<abstract>>
Strategist <<abstract>>
Business Architect <<concrete>>
Database Architect <<concrete>>
Hardware Architect <<concrete>>
Information Architect <<concrete>>
Security Architect <<concrete>>
Software Architect <<concrete>>
System Architect <<concrete>>



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. Concurrent Software Reliability

The importance of software reliability has dramatically increased due to the popularization of concurrent software, because concurrent software is notoriously difficult to develop, and therefore high-quality concurrent software is very costly to produce.

Even further, modern concurrent software is ubiquitous and brings novel challenges for two reasons. On one hand, modern software needs to optimize the use of new multi-core and multi-processor hardware. On the other hand, because many systems are increasingly distributed and must respond to humans in a timely manner. The distributed nature of modern software is both present at a small scale—for example inside our mobile phones—, or at internet scale, for example in social networks and planet-wide

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.

information systems. Modern concurrent software differs from classical approaches to concurrent programming in crucial aspects, like the structure of the synchronization—where large blocks are avoided 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 state explosion undermines the effectivity of testing and leaves verification as a more appealing technique for software reliability.

New verification methods are needed to face the challenges of reliability of modern concurrent software 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, even though automatic verification techniques are desirable because they do not require intervention and can be applied to existing software, it is a big challenge to design automatic techniques that scale to the size of realistic code bases. 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 and distributed data manipulation. Apart from building the foundations to reason rigorously about these aspects of modern concurrent software, this research line also involves 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.

3.5. 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.

3.6. Privacy in the Digital World

The ever increasing data processing and storage capabilities enabled by technological advances open up tremendous opportunities for society, for the economy, and for individuals. However, the collection of massive amounts of electronic data raises concerns regarding the revelation of information that not only results in privacy breaches buy may also impact people's freedom, or create unbalance in power relations which in turn may damage our democratic society. A deep understanding of the implications for privacy of the explosion of, for instance, Big Data analytics, pervasive sensors (e.g., wearables or smartphones), or personalized services (e.g., personalized medicine) is needed in order to fully exploit the benefits of these technologies without harming the fundamental values of our society such as freedom, democracy, or equality.

In this context it is essential to provide ICT system designers with means to consider privacy requirements, as well as with appropriate tools to analyze the privacy properties achieved by their designs. However, we currently lack general methodologies that allow engineers to embed privacy-preserving mechanisms in ICT designs or that allow to test these mechanisms' efficacy. Instead, privacy-preserving solutions are designed and evaluated in an ad-hoc manner, hindering comparison and integration in real-world systems. Furthermore, privacy is typically in conflict with other requirements such as functionality, performance, usability, or cost. Hence, it is necessary to identify means to design systems that meet such 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 to put into practice the "Privacy by Design" paradigm both from the design and evaluation points of view. On the design side the research performed at the Institute involves two aspects. First, researchers work towards the articulation of principles that allow designers and engineers to reason about privacy. Such principles ease the elicitation of privacy requirements, and guide the designer towards best choices of system architechture and

Username:
Administrator
Password:
●●●●●●●●●

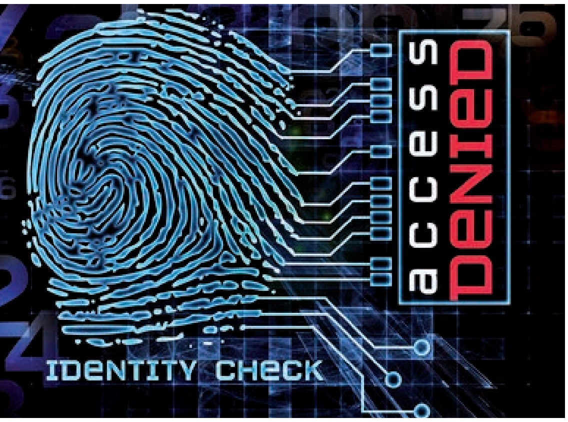
state-of-the-art privacy-preserving technologies when building ICT systems that offer optimal trade-offs between privacy protection and other requirements. A second line of research involves the design of privacy-preserving cryptographic primitives that enable the outsourcing of computations without revealing data in the clear, hence preserving privacy, and the integration of such novel primitives into end-to-end secure systems that achieve concrete functionalities.

With respect to the evaluation of privacy-preserving systems, the research performed at the Institute tackles mainly two challenges. On the one hand the development of meaningful measures and metrics that allow users and analysts to agree on what it means for privacy to be "sufficiently" protected, and on the other hand the development of tools and methods that allow to systematically analyze the privacy protection offered by ICT systems with respect to the developed metrics.

Recent developments at the IMDEA Software Institute in these research directions include tools to study the information leaked by cache memories, a novel method to measure privacy in location-based applications, and a means to prove correctness of a computation over a set of data to a third party without this party learning any information about these data.

3.7. 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.

Researchers at the IMDEA Software Institute are developing novel defenses against cybercrime and targeted attacks. They have launched the commercial CADENCE system for detecting targeted attacks. They have developed novel Internet-wide scanning techniques to detect malicious servers on the Internet. They have proposed deanonymization techniques for malicious servers that may run as hidden services in the Tor anonymity network. And, they have analyzed the abuse by malware and potentially unwanted programs of the Windows code signing solution. This research is being performed in part within the MALICIA and CADENCE projects (see Chapter 5).

3.8. 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 their control 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.

3.9. Computer-Aided Cryptographic Proofs

The goal of modern cryptography is to design efficient algorithms that simultaneously achieve some desired functionality and provable security against resource-bounded adversaries. Over the years, the realm of cryptography has expanded from basic functionalities such as encryption, authentication and key agreement, to elaborate functionalities such as zero-knowledge protocols, secure multi-party computation, and more recently verifiable computation. In many cases, these elaborate functionalities can only be achieved through cryptographic systems, in which several elementary constructions interact. As a consequence of the evolution towards more complex functionalities, cryptographic proofs have become significantly more involved, and more difficult to check. Several cryptographers have therefore advocated the use of tool-supported frameworks for building and

verifying proofs; the most vivid recommendation for using computer support is elaborated in a farseeing article of Halevi that describes a potential approach for realizing this vision.

Besides increasing confidence in cryptographic proofs, tool-supported frameworks have the potential to address another prominent difficulty with provable security: because cryptographic proofs are very complex, it is common practice to reason about algorithmic descriptions of the cryptographic constructions, rather than about implementations. As a consequence, implementations of well-known and provably secure constructions are vulnerable to attacks, and regularly fail to provide their intended security guarantees. This uncomfortable gap between provable security and cryptographic engineering may be due to (i) the mismatch between the powerful but abstract adversary models considered in proofs and "real-world" adversaries that may glean information about the secret data not only from the input and output to computations, but also from a host of side-channels (timing, power consumption or electromagnetic radiations...), and may even be able to interfere with the computation itself; (ii) the fact that the object on which the security proof is performed is not the object that is implemented in practice, either due to a developer's (possibly malicious) mistake or even to an unjustified refinement when turning abstract algorithms into standard documents and recommendations. These points are the focus of the recent "real world" security approach to provable security, developed, most notably by Degabriele, Paterson, and Watson.

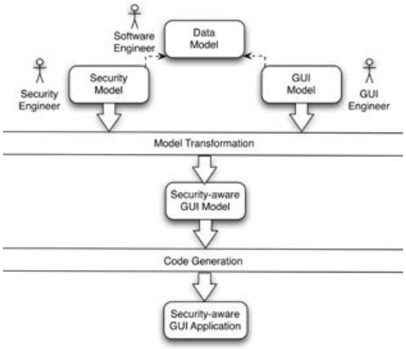
Researchers at IMDEA are actively working on developing foundations and proving tool support for building and verifying the security of cryptographic constructions. To date, they constructed several tools, ranging from general frameworks that can be applied to many classes of constructions to specialized frameworks which target a single class of constructions, or tool for automatically analyzing and synthesizing secure instances within well-defined classes of cryptographic constructions.

3.10. Model-Driven Data Security and Privacy Management

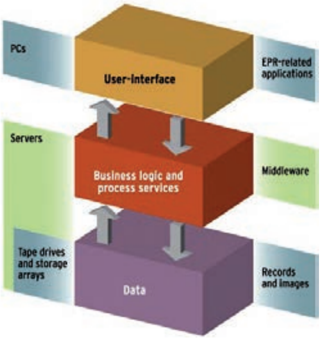
The derivation of code from models (model-driven software development) offers the advantage of automating the coding of at least certain parts of applications, an approach which can avoid the introduction of errors that is frequent in manual software production. IMDEA Software researchers are applying 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.

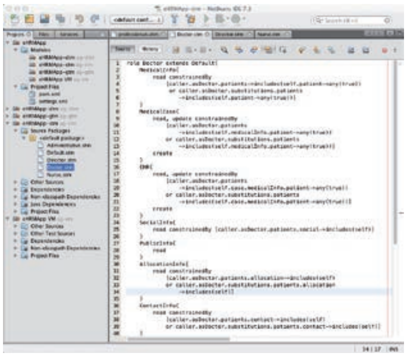
Researchers at the IMDEA Software Institute, in collaboration with ETH Zurich, have developed a novel model-driven methodology for developing secure data-management applications. System developers proceed by modeling three different views of the desired application: its data model, security model, and 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



Model-driven development of security-aware GUIs.



3-tier architecture

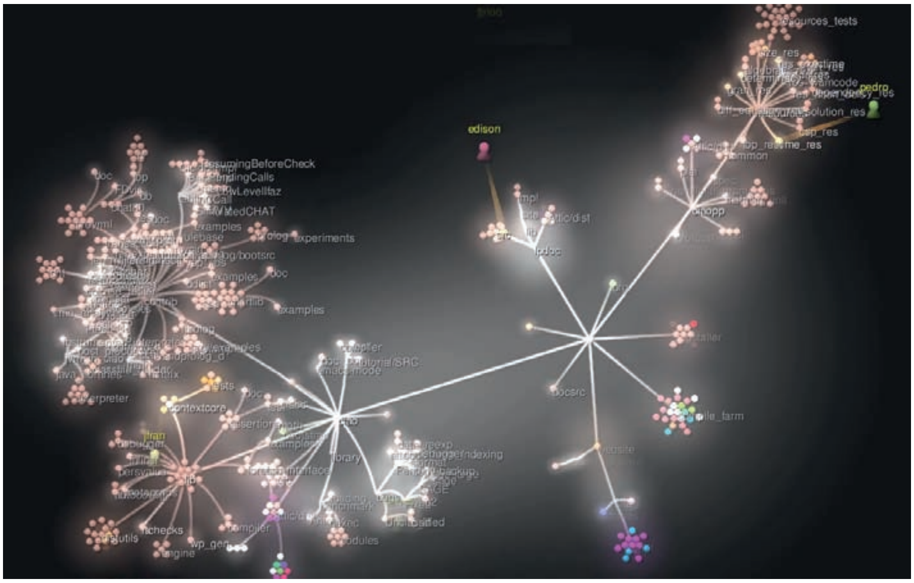


```
role Doctor extends Default{
    MedicalInfo{
        read constrainedBy
            [caller.asDoctor.patients->includes(self.patient->any(true))
             or caller.asDoctor.substitutions.patients
                ->includes(self.patient->any(true))]
    }
    MedicalCase{
        read, update constrainedBy
            [caller.asDoctor.patients
                ->includes(self.medicalInfo.patient->any(true))
            or caller.asDoctor.substitutions.patients
                ->includes(self.medicalInfo.patient->any(true))]
        create
    }
    EHR{
        read, update constrainedBy
            [caller.asDoctor.patients
                ->includes(self.case.medicalInfo.patient->any(true))
            or caller.asDoctor.substitutions.patients
                ->includes(self.case.medicalInfo.patient->any(true))]
        create
    }
    SocialInfo{
        read constrainedBy [caller.asDoctor.patients.social->includes(self)]
    }
    PublicInfo{
        read
    }
    AllocationInfo{
        read constrainedBy
            [caller.asDoctor.patients.allocation->includes(self)
            or caller.asDoctor.substitutions.patients.allocation
                ->includes(self)]
    }
    ContactInfo{
        read constrainedBy
            [caller.asDoctor.patients.contact->includes(self)
            or caller.asDoctor.substitutions.patients.contact->includes(self)]
    }
```

ActionGUI: An example of a security model (screenshot) 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.



people

4

annual report
2015

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.

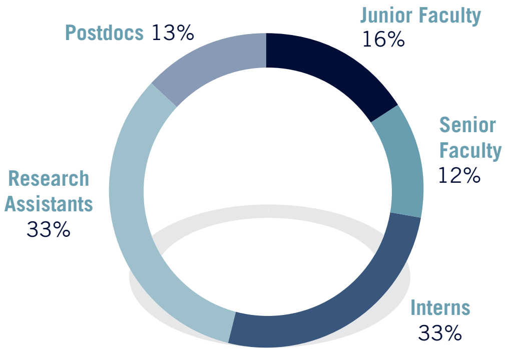


Figure 4.1. Type of position, all researchers.

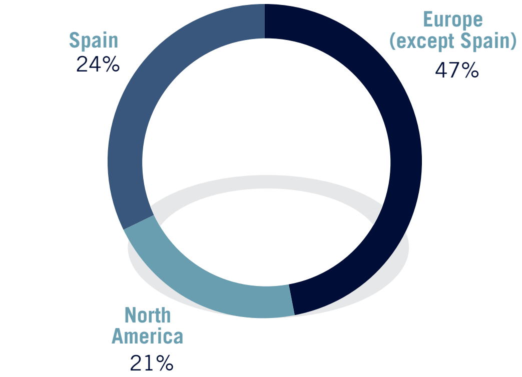


Figure 4.2. Where PhD was obtained (by continent + Spain).

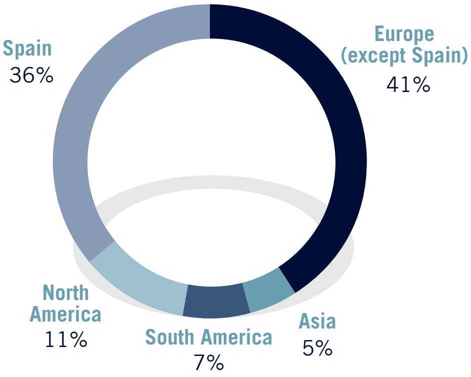


Figure 4.3. Location of previous institution, all (by continent + Spain).

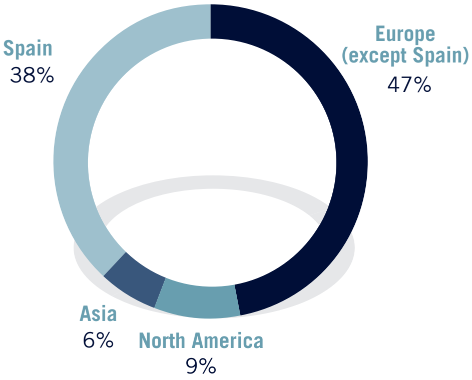


Figure 4.4. Nationality of researchers at or above postdoc level (by continent + Spain).

Status

In 2015, the scientific staff of the Institute was composed of ten senior faculty (full or associate professors, one part-time), thirteen junior faculty (tenure-track or researchers), ten postdoctoral researchers, twenty six research assistants (PhD candidates), twelve project staff, three system support staff, and five administrative support staff (three part-time). Four senior faculty visitors and twenty one interns spent a variable length of time (from one month to a year) at the Institute collaborating with faculty members. Figure 4.1 shows the proportions of each category at the end of 2015 (where 28% were faculty members vs. 72% non-faculty). Figure 4.2 summarizes where these researchers obtained their PhD (by continents plus Spain), and Figure 4.3 shows the location where the Institute researchers were working previously to joining IMDEA. Finally, Figure 4.4 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 a member of the scientific boards of INRIA and Dagstuhl, among others. 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 is also one of the most cited Spanish authors in Computer Science. 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 and CLC Manager and Scientific Coordinator of the Madrid node of EIT Digital. 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. Anindya is currently on leave from the Institute at NSF.

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.

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 a Ph.D. degree in Computer Science from Stanford University, USA, in 2007. His thesis studies the 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. He become a Scientific Researcher at the Spainish 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, granted 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 was the 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 interests are based on the applications of logic, games and automata theory for the development, the understanding, and the verification of computational devices. In particular, Cesar's main line of research is the use of 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 and distributed systems, runtime verification, and specification languages to express rich properties of modern concurrent software systems.

Pierre Ganty

Associate Research Professor

Pierre is a 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

Associate 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. His Ph.D. thesis received a Best Dissertation Award of the European Association for Programming Languages and Systems (EAPLS). Alexey 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.

Research Interests

Alexey’s research interests are in developing programming models, methods and tools for developing correct concurrent and distributed software.

Boris Köpf

Assistant Research Professor

Boris joined the IMDEA Software Institute in 2010 after completing a Ph.D. in the Information Security group of ETH Zurich and working as a postdoc at the Max Planck Institute for Software Systems. 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. He is an alumnus of the German National Academic Foundation and holds a Ramón y Cajal fellowship.

Research Interests

Boris is working on principled techniques for reasoning about security/performance tradeoffs in software systems. The goal of his work is to provide engineers with practical tools to tap unexplored performance potentials while retaining adequate degrees of security.

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. His research focuses mainly on designing provably-secure cryptographic protocols, and his recent work has particular emphasis on developing novel paradigms that provide security to 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, 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 Università 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 interested in the formalization of mathematics, the formal study of *Differential Power Analysis* counter-measures, and is 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.

Benedikt Schmidt

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.

Alley Stoughton

Researcher

Alley Stoughton received her PhD in computer science from the University of Edinburgh in 1987. Her doctoral research was on the “full abstraction” problem for programming language semantics. From 1986 until 1993, she was a research fellow and then a lecturer at the University of Sussex, where she developed an interest in implementing logic-based tools. In 1993, she joined Kansas State University as an associate professor, where she expanded her research to include functional programming. While at K-State, she designed and implemented Forlan, an open-source toolset for experimenting with formal language theory. From 2012 until 2015, she was a member of the technical staff of MIT Lincoln Laboratory, focusing on the application of formal methods and programming languages to cyber security. She joined IMDEA’s Computer-Assisted Cryptography Group in 2015.

Research Interests

Alley’s research applies formal methods and programming languages to cyber security. With other members of IMDEA’s Computer-Assisted Cryptography Group, she is formalizing in EasyCrypt the security of NIST’s SHA-3 secure hash algorithm standard. She is also using EasyCrypt to prove the security of private information retrieval cryptographic protocols. And she is researching the application of theoretical cryptography’s real/ideal paradigm to the security of programs.

Carmela Troncoso

Researcher

Carmela received her Ph.D. in Engineering from the KU Leuven in 2011, where she was a student at the COSIC Group. Her thesis “Design and Analysis methods for Privacy Technologies”, advised by Prof. Bart Preneel and Prof. Claudia Diaz, received the ERCIM WG Security and Trust Management Best Ph.D. Thesis Award. During her PhD Carmela was a research visitor at many well-known security groups, including a three-month internship at Microsoft Research’s lab in Cambridge, UK. After a year of post-doc at KULeuven she joined Gradiant, the Galician R&D Center in Advanced Telecommunications, where she became the Security and Privacy Technical Lead. At Gradiant Carmela worked on secure and private practical solutions with local and international companies, filing one patent on vehicle-to-cloud secure communications. In October 2015 Carmela joins the IMDEA Software Institute as Researcher.

Research Interests

Carmela’s main interest is privacy research. Her work tackles mainly two aspects: how to build privacy-preserving systems and how to help engineers embedding strong privacy guarantees in their designs; and how to develop techniques to systematically quantify the private information that an adversary can infer from data she may have access to. Recently, she has become very interested in genomic privacy, and in finding solutions to enable safe sharing of genetic data.

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.

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 University of Madrid.

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 a BSc and MSc in computer science from Ca'Foscari, the University of Venice. During his master he spent one year studying bioinformatics at the University of Leiden. Giovanni obtained the PhD from Trinity College Dublin, and after two Post-Docs, one in Dublin, and a short one at the Universidade de Lisboa, he arrived at IMDEA Software.

Research Interests

Giovanni is interested chiefly in operational and denotational semantics of programming languages for concurrent software, and in type systems for concurrency. His PhD thesis unravels a series of behavioural equivalences for clients and peers within two settings, the Calculus of Communicating Systems, and higher-order session types. In subsequent work he constructed a fully-abstract semantic explanation of the standard subtyping for session types, and questioned the existing notions of duality for these types. At IMDEA Software he is working on the foundations of weak consistency levels for distributed databases, and on robustness criteria for them.

Alejandro Sanchez

Postdoctoral researcher

After obtaining his BSc in Computer Science from the National University of Córdoba in Argentina, Alejandro joined the IMDEA Software Institute in 2009, first as a research intern and later as a PhD Student. In 2011, he obtained his MSc in Programming and Software Technology from the Complutense University of Madrid and more recently, in September 2015, he obtained his PhD in Computer Science from the Technical University of Madrid.

Research Interests

Alejandro's main research interest is the formal verification of temporal properties of safety and liveness on concurrent systems that dynamically manipulate pointer-based data structures in the heap. He is particularly interested in the formalization, development and implementation of innovative deductive verification techniques, theories and decision procedures capable of dealing with the verification of rich properties in concurrent programs, with a special emphasis on parametrized systems.

Pablo Nogueira

Postdoctoral researcher

Pablo Nogueira has joined the IMDEA Software Institute in mid November 2015. He holds a PhD in Computer Science from the University of Nottingham, United Kingdom, where he was funded by a studentship from the School of Computer Science and Information Technology. His thesis supervisor was Professor Roland C. Backhouse. From 2010 to 2015 he was an Assistant Professor at ETSI Informáticos, Universidad Politécnica de Madrid, where he lectured and coordinated several graduate and postgraduate courses such as Algorithms and Data Structures and Functional Programming. Before that, he held post-doctoral positions and research fellowships in Spain and the United Kingdom.

Research Interests

His research interest at large is on the theory and practice of programming and programming languages, their foundations, applications, implementations, and tools. Pablo has worked on varied topics such as generic functional programming, abstract data types and category theory, proof-directed debugging, relational algebra and unification, verification and optimisation by program transformation, operational semantics, and lambda calculi. His latest work has focused around lambda calculi and program transformation. He is also working with Associate Research Professor César Sanchez in program transformation and abstraction for fine-grained concurrent data structures.

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

Bogdan Warinschi
Visiting Professor

University of Bristol, UK

Visiting during
Apr. 2015 – Jul. 2015

Somesh Jha
Visiting Professor

University of Wisconsin, USA

Visiting during
Sep. 2015 – Jun. 2016

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).

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.

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.

Antonio Nappa

Research Assistant

Degree: Università degli Studi di Milano, Italy

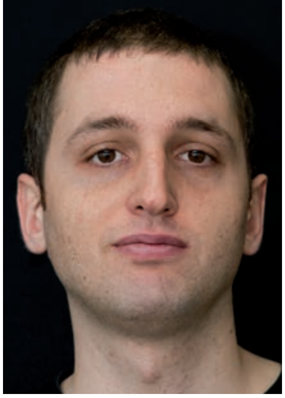
Research: Investigating two fundamental aspects of cybercrime: vulnerability patch deployment and malicious infrastructures detection.

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.

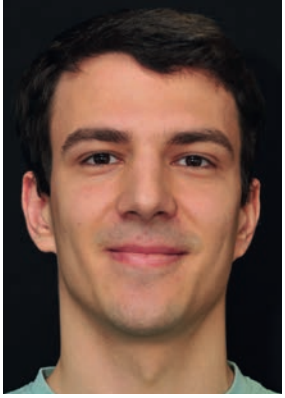


Goran Doychev

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.



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).

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

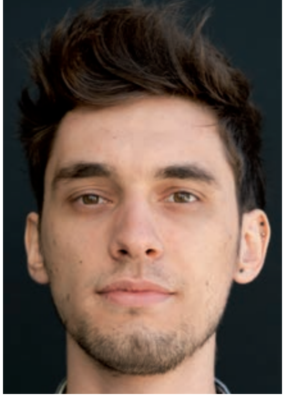
Research: Abstract interpretation-based static analysis for inferring energy consumption information about (concurrent) program executions. He is working on the FP7 project "Whole-Systems ENergy TRAnsparency" (ENTRA).

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: M.Sc. in Mathematics, 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: Malware Unpacking, Binary Analysis, Web Security.

Raul Alborodo

Research Assistant

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

Research: Formal methods applied to concurrent programming, software specification and verification, model-driven methodologies, concurrent programming based on shared resources.

Platon Kotzkias

Research Assistant

Degree: M.Sc in Digital Systems security University of Piraeus, Greece.

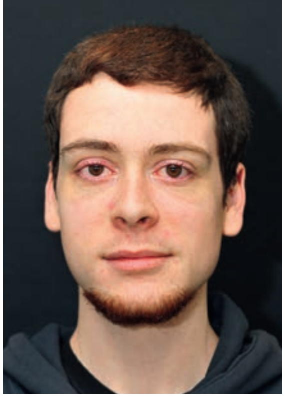
Research: System security, malware analysis, network security, cybercrime.

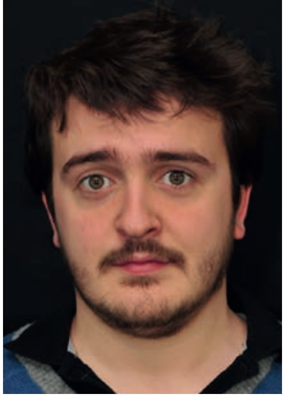
Richard Rivera

Research Assistant

Degree: Engineering in Information Systems and Computing, Escuela Politécnica Nacional(EPN), Ecuador. MSc in Software and Systems, Technical University of Madrid (UPM), Spain.

Research: Malware analysis and classification, cybercrime, machine learning applied to security, development and optimization of malware analysis environments.





Luthfi Darmawan
Research Assistant

Degree: Universidad Politecnica de Madrid (UPM), Spain

Research: Resource usage verification of computer programs.

Pablo Cañones
Research Assistant

Degree: Universidad Complutense de Madrid (UCM), Spain

Research: Information theory and security guarantees for cryptographic processes, targetting the security against side channel attacks through hardware architecture.

Martín Moreau
Research Assistant

Degree: MSc in Numeric Security Reliability and Performance, Université Pierre et Marie Curie (UPMC), Paris, France

Research: Cryptography and the verification of its implementation as well as the analysis of side-channel attacks and their countermeasures.

Paolo Calciati
Research Assistant

Degree: Università della Svizzera Italiana, Lugano, Switzerland

Research: Improve quality and security of mobile applications using automated testing and malware detection techniques.

Giuseppe Guagliardo
Research Assistant

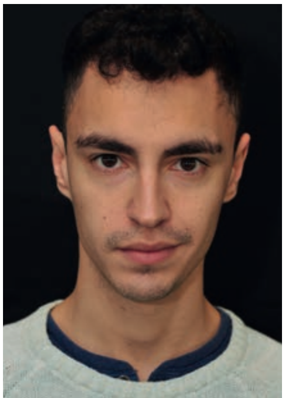
Degree: Université de Bordeaux, Bordeaux, France

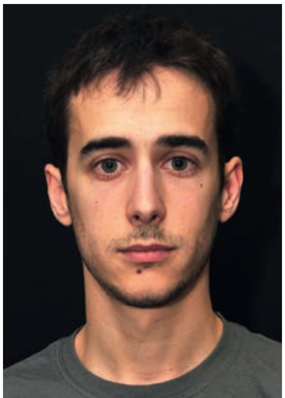
Research: Cryptography and Provable Security with emphasis on Public Key Exchange Protocols. Computer aided security proofs with focus on Game theoretic techniques.

Pepe Vila
Research Assistant

Degree: Before joining IMDEA Software in November 2015, Pepe studied Computer Engineering at the Universidad de Zaragoza and worked as a security consultant/penetration tester for an international firm.

Research: Currently he is working on his PhD on computer security, and his research interests include web application security, specially client-based web browser attacks (and countermeasures), NFC security and side-channel attacks.





interns

Intern	Period	Nationality
Marcos Sebastián	Oct. 2014 – Mar. 2016	Spain
Elena Gutierrez	Jun. 2015 – Feb. 2016	Spain
Victor de Juan	Jun. 2015 – Jan. 2016	Spain
Pedro Valero	Sep. 2015 – Feb. 2016	Spain
Ignacio Queralt	Sep. – Dec. 2015	Spain
Cecile Baritel	Oct. 2015 – Aug. 2016	France
Massimo Neri	Oct. 2015 – Jan. 2016	Italy
Anca Nitulescu	Mar. – Sep. 2015	Romania
Santiago Cervantes	Sep. 2014 – Sep. 2015	Spain
Alejandro Ranchal	Sep. 2014 – Sep. 2015	Spain
Renzo Verastegui	Jun. 2015 – Apr. 2016	Romania
Santiago Cuellar	Jul. – Sep. 2015	Colombia
Xavier Garceau-Aranda	Jun. – Sep. 2015	Spain
Daniel Henri-Mantilla	Jun. – Aug. 2015	Spain
Justin Hsu	May – Jul. 2015	United States
Leo Stefanesco	May – Aug. 2015	France
Simón Cancela	Oct. 2014 – Jul. 2015	Spain
Thomas Espitau	Mar. – Aug. 2015	France
Guillermo Ramos	Jul. 2013 – Jun. 2015	Spain
Rana Faisal Munir	Nov. 2014 – Feb. 2015	Pakistan
Pablo Rauzy	Jan. – Feb. 2015	France

project staff and technology transfer unit

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.

Jesús Contreras

Business Developer, EIT Digital & Project Strategy Manager

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

Juan José Collazo

Project Manager, AMAROUT-II

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

Francisco Ibáñez

Business Developer, EIT Digital

Degree: MBA Finance & Entrepreneurial Management - Harvard Business School, USA

Susana Eiroa

Doctoral Training Center Lead, EIT Digital

Degree: PhD in Microelectronics – IMSE-CNM-CSIC, Universidad de Sevilla, Spain

Andrea Iannetta

Administrative Assistant, EIT Digital

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

Silvia Díaz-Plaza

Project Assistant, N-GREENS

Degree: B.Sc. in Administration and Business Management - Universidad Rey Juan Carlos, Madrid, Spain

David García

Social Media & Web Manager, EIT Digital

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

Leandro Guillén

Technical Project Staff, Telefónica Joint Research Unit

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

Guillermo Jiménez

Technical Project Staff, Telefónica Joint Research Unit

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

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

REDIMadrid staff

David Rincón

REDIMadrid Network Engineer

Degree: BS in Telecommunications - Technical University of Valladolid, Spain

Carlos Ricardo de Higes

REDIMadrid Technician and Computer Operations

Degree: Licensed Electrical Technician, Instituto Juan de la Cierva, Madrid, Spain

Carlota Gil

Accounting Assistant

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

Begoña Moreno
IMDEA Common Services (part-time)

Degree: Ph.D. in Economics and Political Sciences

Laura Bellmont
Infrastructure Manager

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

research projects and contracts

5

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 2015, the Institute participated in a total of 30 funded research projects and contracts, the majority of which (23, the 77%) involve collaboration with industry. Of the 30 projects, 19 are from international agencies (16 funded by the European Union and 3 by the US agencies ONR and NIST), 5 of them are direct industrial funding, and the rest are funded by national (5) and regional (1) agencies. Figure 5.1 shows the origin of project funding. In the same year, the Institute benefited from 14 fellowships.

The trend of external funding for the period 2008-2015 is shown in Figure 5.2 (the value for 2015 is estimated and that for 2016 is a forecast). The amount of external funding (and the percentage of external to total funding) has risen from around 1.1 M€ (30%) in 2013 to 1.8 M€ (42%) in 2015, which is slightly above the forecast for 2015 performed at the end of 2014 (1.75 M€), partially due to activities performed in the realm of EIT Digital. The level of external funding is forecast to grow to 1.9M€ in 2016, with the percentage of external funding with respect to the total Institute budget rising to 47%.

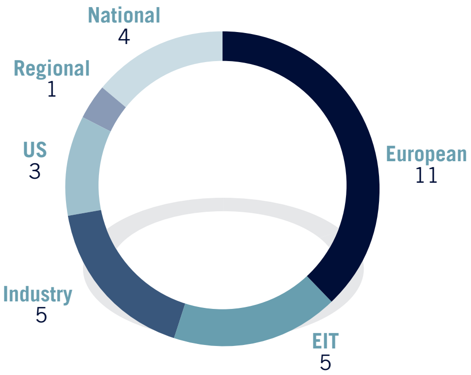


Figure 5.1. Projects by origin of funding.

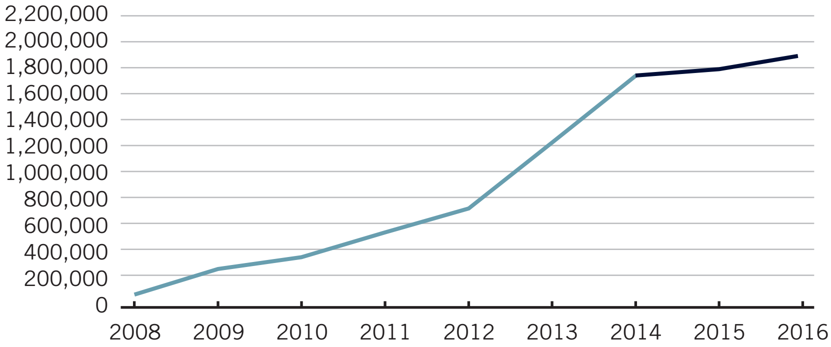


Figure 5.2. Evolution in external funding since 2008.

5.1. Projects Running in 2015

SynCrypt

Automated Synthesis of Cryptographic Constructions

Funding: US Office of Naval Research (ONR), through Stanford University
Duration: 2015-2018
Project Coordinator: Res. Prof. Gilles Barthe

SynCrypt is a joint project with Stanford University, University of Pennsylvania, and SRI, funded by ONR and which runs from September 2015 until August 2018. SynCrypt is the continuation of AutoCrypt project and the budget allocated for IMDEA Software is over 1 Million Euros. SynCrypt aims to develop synthesis techniques and tools for cryptographic constructions, and for cryptographic implementations. Building on their previous work, IMDEA researchers will develop synthesis tools for generating, transforming, and hardening cryptographic constructions.

Within the project, the IMDEA Software team plans to extend their EasyCrypt tool (http://www.easycrypt.info) to handle proof generation for lattice-based systems. This will require a fair amount of enhancements to EasyCrypt. IMDEA will extend the logical rules for proving security of cryptosystems to reason about noise growth and will apply these tools to analyze lattice-based identity-based systems and attribute-based encryption schemes.

SHA3

Verified standards: SHA3

Funding: US National Institute of Standards and Technology (NIST)
Duration: 2015-2016
Project Coordinator: Res. Prof. Gilles Barthe

SHA3 research project is funded by NIST and runs from September 2015 until August 2016. The goal of the project is to demonstrate that the EasyCrypt tool can be used for building machine-checked, independently verifiable proofs of security for the new SHA3 standard.

The technical work will be performed in two steps. IMDEA researchers shall first consider indifferentiability from a random oracle, which is among the strongest properties for hash functions and extendable-output functions, and will formalize a detailed game-based proof of indifferentiability in EasyCrypt for the sponge construction used in the SHA3 standard.

Finally, the IMDEA Software team will generate a C implementation from the formalization, and validate the correctness of the implementation experimentally.

EIT Digital Spain APG

APG Spain EIT Digital Coordination and Joint Activities

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2015-2016
Principal Investigator: Res. Prof. Manuel Hermenegildo

EIT Digital, as explained in section 2.3, is the Knowledge and Innovation Community (KIC) in the ICT sector of the European Institute of Innovation and Technology. The Spanish node is currently the last one to join the KIC. The Spanish node, formalized through the Associate Partner Group Spain (APG Spain), includes the following members: IMDEA Software Institute (node coordinator), Technical University of Madrid, ATOS, Indra, Telefónica, and the Barcelona Supercomputing Center. The coordination includes boosting the network in collaboration with members of APG with a twofold objective. On one hand to improve knowledge of the KIC possibilities in order to take maximal profit from the innovation program. On the other hand to spread the activities of the APG in the national ICT sector at all levels: large companies, SMEs, entrepreneurs, students, academia and researchers. This project aims at providing support for these coordination activities in order to strengthen the position of Spain in EIT Digital.

CADENCE

Cyber Attack Detector Engineering for Commercial Exploitation

Funding: European Institute of Innovation and Technology
Duration: 2015
Principal Investigator: Asst. Res. Prof. Juan Caballero

The CADENCE project is an action part of the EIT Digital activities in 2014 and 2015 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. More information appears in Chapter 7.

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 Future Internet PPP (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 network of EIT Digital hubs in Budapest, Eindhoven, Helsinki, Madrid, Paris, and Trento, where nodes of EIT Digital have their co-location centers. 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.

FI-CORE

Funding: European Union – 7th Framework Program
Duration: 2014–2016
Principal Investigator: Res. Prof. Manuel Hermenegildo

The FI-Core project aims to complete the FI-PPP vision and support a truly open innovation ecosystem around FIWARE Lab, a working instance of FIWARE that is distributed across multiple data centers in Europe and is effectively operated using the suite of FIWARE Ops tools. In this project, the FI-Core consortium is delivering:

- Technology extensions, introducing new capabilities to the platform, with focus on those believed to carry substantial economic potential and future relevance. Examples include new Generic Enablers (GEs) in the areas of Robotics, Open Data, and Network Function Virtualization.

- Means for platform availability, including initiatives and processes for ensuring the effective adoption of FIWARE GE's well beyond the initial FI-PPP community. These means include the launch of operational FIWARE nodes across Europe with resources and tools to support them, as well as extensive FIWARE education and training programs for Web entrepreneurs and SMEs.

- Processes and tools for platform sustainability, ensuring outreach and dissemination of current and on-going results from FI-Ware and Xifi projects, and their take-up by the European and global ecosystems, based on the large involvement of SMEs which will use the platform to create new value networks.

N-GREENS

Next-Generation Energy-Efficient Secure Software

Funding: Regional Government of Madrid
Duration: 2014–2018
Project Coordinator: Res. Prof. Gilles Barthe

Comunidad de Madrid

POLITÉCNICA

UNIVERSIDAD COMPLUTENSE MADRID

The N-GREENS Project 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. N-GREENS 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: 2013–2015
Principal Investigator: Asst. Res. Prof. Pavithra Prabhakar

The VeriStab project addresses the challenge of building high-confidence embedded control systems by 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 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 which covers from the development of 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 (http://advent-project.eu). 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 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.

Polca

MAXELER Technologies
MAXIMUM PERFORMANCE COMPUTING

RECORE

cetic

ulm university universität uulm

UNIVERSITY OF TWENTE.

Universität Stuttgart

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

Automation in Cryptology

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.

VARIES

Variability in safety critical embedded systems

Funding: ARTEMIS- European Union - 7th Framework Program
Duration: 2012-2015
Principal Investigator: Assoc. 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.

StrongSoft

Sound Technologies for Reliable, Open, New Generation Software

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2013–2016
Principal Investigator: Assoc. 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.

e-TUR2020

e-TUR2020. TUrismo & Retail

Funding: Spanish Ministry of Economy and Competitiveness - CDTI
Duration: 2015-2019
Principal Investigator: Asst. Res. Prof. Juan Caballero

e-TUR2020 is a 4-year Spanish joint industrial research project funded by the Centre for the Development of Industrial Technology (CDTI). The aim of e-TUR2020 is to create a new on-line platform for the tourism sector that will enrich the sector's mobile applications with new services for tourists, tourist sector agents, and companies from other sectors. The e-TUR2020 project involves 6 industrial partners (Compartia, Eurona, Groupalia, SoluSoft, Tecnocom, Zemsania). The industrial partners subcontract parts of the work to 4 research and development centers (Eurecat, IMDEA Software Institute, PCT, and Universidad Carlos III de Madrid). Within e-TUR2020, the IMDEA Software Institute will manage the security aspects. To this end, the Institute will contribute to research and develop techniques to secure the information exchange.

ARVI

Runtime Verification Beyond Monitoring

Funding: European Union, COST Action
Duration: 2014–2018
Investigator: Assoc. 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: Asst. 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 researchers 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.

EUIN Grants

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2015

Europa Investigación Grants, funded by MINECO, support the submission of proposals from Spanish research groups to calls belonging to the H2020 Framework Programme. IMDEA Software has obtained three of these grants to support the submission of three research proposals to the European Research Council (for Consolidator Grants and Starting Grant, made by Pavithra Prabhakar, Alexey Gotsman and Aleksandar Nanevski) in 2015.

EIT Digital CLC

Co-Location Center

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

EIT Digital Business Development Accelerator

The Digital Business Development Accelerators (BDAs) are part of the EIT Digital BDA network, and provide 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. In 2015 the business acceleration activities of the Madrid APG led by the IMDEA Software Institute have been expanded (from one person to two people) with a new additional expert Francisco Ibáñez establishing relationships with the Spanish venture capital and investment ecosystems.

EIT Digital Higher Education Schools

During 2015, the Spanish APG, led by the IMDEA Software Institute, started the EIT Digital Doctoral and the Master School. The first 20 students of the the EIT Digital Master School started innovation and entrepreneurship lectures at the Co-location Centre (CLC) in the IMDEA Software premises. In the Doctoral School, the first six PhD students started the EIT Digital program attending the first courses (Raising Awareness), also at the Co-Location Center in the IMDEA Software Institute.

eit Digital

Telefónica
Investigación y Desarrollo

Atos

indra

POLITÉCNICA

BSC Barcelona Supercomputing Center
Centro Nacional de Supercomputación

Microsoft Research

The strong cooperation between scientists in IMDEA Software and Microsoft Research was boosted through the opening of the Joint Research Center and the organization of the Microsoft Research and IMDEA Software Institute Cooperation Workshops (MICW). 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. On April 9-10, 2015 the second edition of the Microsoft Research and IMDEA Software Institute Collaboration Workshop (MICW 2015) took place, focused on three main topics: Scalable and correct data management in the cloud, verification for cryptography and security, and secure Distributed Programming. MICW 2015 aimed at discussing collaborative work on chosen software projects and, when possible, to bring those advances to Microsoft's businesses.

Telefónica I+D

Since 2012, IMDEA Software has cooperated with *Telefónica I+D* on research and development of 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, Telefónica Digital and the Institute also established during 2013 a *Joint Research Unit* (JRU) within their more global strategic partnership.

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.

5.2. Some Recently Granted Projects (not started in 2015)

NEXTLEAP

NEXt Generation Technosocial and Legal Encryption Access and Privacy

Funding: European Union - H2020 Framework Program
Duration: 2016-2018
Project Investigator: Asst. Res. Prof. Dario Fiore

The objective of the NEXTLEAP project is to build the fundamental interdisciplinary internet science necessary to create decentralized, secure, and rights-preserving protocols for the next generation of collective awareness platforms. The longterm goal of NEXTLEAP is to have Europe take the “next leap ahead” of the rest of the world by solving the fundamental challenge of determining both how to scientifically build and help citizens and institutions adopt open-source, decentralized and privacy-preserving digital social platforms. This paradigm is in contrast to proprietary, centralized, cloud-based services and pervasive surveillance that function at the expense of rights and technological sovereignty.

TRACES

Technologies and tools for Resource-Aware, Correct, Efficient Software

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2016-2018
Project Investigators: Assoc. Res. Prof. Manuel Carro - Res. Prof. Manuel Hermenegildo

The focus of TRACES Project relies in the need of change in the fundamental tools and approaches which underlie the software engineering techniques to be applied in the very near future. For this purpose TRACES includes three main research lines: 1) Resource-aware computing: being able to determine safe (or at least approximate) bounds for the resource consumption of software in a given hardware, and optimize it as much as possible, is necessary to ensure the correctness of embedded devices in terms which are more general than just functional correctness. 2) Advanced techniques to ensure functional correctness: these include not only infinite-state verification, but also debugging, synthesis of concurrent software, probabilistic / heuristic methods, and lean methods, such as testing and runtime / dynamic verification. These are necessary when, for example, the boundaries of a computer system are not well known in advance, or the interactions with the outside world can only be probabilistically modeled. 3) New language technologies: new environments, tasks, and missions make it necessary to adapt existing languages to them or to create languages anew. Contrary to widespread belief, new languages and programming models are constantly created not only in academia but also in industry with the aim of either taking advantage of new devices or of performing tasks (e.g., knowledge-related) which would be too complex to write (and to ensure correct!) in traditional languages.

DEDETIS

Detecting and Defending Against Threats to the Information Society

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2016-2018
Project Investigators: Asst. Res. Prof. Juan Caballero - Asst. Res. Prof. Boris Köpf

The goal of the DEDETIS project is to deliver the next generation of detection and defense techniques and tools against cyber threats. While our techniques and tools will be useful in multiple application scenarios, the emphasis of the project is on protecting the booming mobile and cloud computing environments against today's and tomorrow's threats. The work plan of the project is organized in 3 research lines that cover: 1) The fight against cybercrime, including novel system and network security approaches for detecting malicious software (malware) in mobile devices, classifying and recovering the software lineage of malware, and disrupting malicious server infrastructures hosted on cloud hosting services. 2) The detection and analysis of software vulnerabilities, including novel program analysis techniques to detect vulnerabilities with high coverage as well as algorithmic vulnerabilities, e.g., side-channel attacks on cryptographic modules and denial of service attacks through resource starvation. 3) Privacy and integrity in cloud computing, including novel cryptographic protocols based on homomorphic encryption and zero-knowledge verifiable computation to securely outsource data and computations to untrusted cloud service providers.

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

RISCO

Rigorous Technologies for the Analysis and Verification of Sophisticated Concurrent Software

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2016-2018
Project Investigators: Assoc. Res. Prof. Pierre Ganty - Asst. Res. Prof. Alexey Gotsman

The overall goal of the project is to develop new foundations for production and rigorous formal reasoning about modern concurrent and distributed computations. Formally proving that concurrent and distributed programs behave as expected is an old problem, and many of its facets have been well understood. However, modern applications, hardware platforms and language standards, keep imposing new and stringent requirements on the development and deployment of such programs. The specific goal of this project is to bridge the gap between the low-level details essential to implementation of programs on modern concurrent and distributed architectures, and the high-level understanding necessary for formal verification. We will tackle the problems using a two-pronged approach, as follows: 1) We will study how the gap can be bridged in an automated way, by investigating complexity of the verification problems for the above modern concurrent and distributed computational models. We will design efficient decision procedures for reasoning about high-level abstract data types in such models, and implement them in tools. 2) We will study how the gap can be bridged in the context of human-assisted (i.e., interactive) proof development. In that setting, the challenge is to come up with proof abstractions that reduce the number and complexity of the required proof obligations, thus enabling humans to develop the correctness proofs by hand.

5.3. Fellowships

1. *Microsoft Research PhD Scholarship funds* (2), active in 2012-2015 (**Alexey Gotsman** and **Boris Köpf**).

2. *Juan de la Cierva Postdoc Incorporación grant*, Spanish Ministry of Science and Innovation, awarded in 2015 and ending in 2017 (**Dario Fiore**).

3. *Ramón y Cajal grant*, Spanish Ministry of Science and Innovation, awarded in 2010 and ending in 2015 (**Aleksandar Nanevski**).

4. *Ramón y Cajal grant*, Spanish Ministry of Science and Innovation, awarded in 2015 and ending in 2020 (**Boris Köpf**).

5. *Marie Curie AMAROUT II Incoming Fellowships (8)*, European Union – 7 Framework Program, awarded in 2012 and active in 2015 (**Dario Fiore**, **Michael Emmi**, **François Dupressoir**, **Benedikt Schmidt**, **Pierre-Yves Strub**, **Ilya Sergey**, **Giovanni Bernardi** and **Alessandra Gorla**).

6. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, active in 2015 (**Miriam García**).

7. *FPU Doctoral Grant*, Spanish Ministry of Education, Culture and Sports, awarded in 2012 and ending in 2015 (**Julián Samborski-Forlese**).

dissemination of results

6

6.1. Publications

6.1.1. Refereed Publications

Journals

1. *Nataliia Stulova*, *José Francisco Morales*, *Manuel Hermenegildo*. *Practical Run-time Checking via Unobtrusive Property Caching*. Theory and Practice of Logic Programming, 31st Int'l. Conference on Logic Programming (ICLP'15) Special Issue, Vol. 15, Num. 04-05, pages 726–741, Cambridge U. Press, September 2015.

2. *Goran Doychev*, *Boris Köpf*, *Laurent Mauborgne*, Jan Reineke. *CacheAudit: A Tool for the Static Analysis of Cache Side Channels*. ACM Transactions on Information and System Security (TISSEC), Vol. 18, Num. 1, pages 1–32, ACM, June 2015.

3. *Giovanni Bernardi*, Hennessy, Matthew. *Mutually Testing Processes*. Logical Methods in Computer Science, Vol. 11, Num. 2, April 2015.

4. *Antonio Nappa*, M. Zubair Rafique, *Juan Caballero*. *The MALICIA Dataset: Identification and Analysis of Drive-by Download Operations*. International Journal of Information Security, Vol. 14, Num. 1, pages 15–33, Springer Berlin Heidelberg, February 2015.

5. *Zorana Bankovic*, *Pedro Lopez-Garcia*. *Stochastic vs. Deterministic Evolutionary Algorithm-based Allocation and Scheduling for XMOS Chips*. Neurocomputing, Vol. 150, pages 82–89, Elsevier, February 2015.

6. Andreas Metzger, Philip Leitner, *Dragan Ivanovic*, Eric Schmieders, Roslin Franklin, *Manuel Carro*, Schahram Dustdar, Klaus Pohl. *Comparing and Combining Predictive Business Process Monitoring Techniques*. System, Man, and Cybernetics: Systems, IEEE Transactions on, Vol. 45, Num. 2, pages 276–290, February 2015.

7. *José Francisco Morales*, *Manuel Carro*, *Manuel Hermenegildo*. *Description and Optimization of Abstract Machines in a Dialect of Prolog*. Theory and Practice of Logic Programming, Vol. FirstView, pages 1–58, Cambridge University Press, January 2015.

8. Beta Ziliani, Derek Dreyer, Neelakantan R. Krishnaswami, *Aleks Nanevski*, Viktor Vafeiadis. *Mtac: A Monad for Typed Tactic Programming in Coq*. Journal of Functional Programming (JFP), Vol. 25, 2015.

9. Antonio Carzaniga, *Alessandra Gorla*, Nicolò Perino, Mauro Pezzè. *Automatic Workarounds: Exploiting the Intrinsic Redundancy of Web Applications*. ACM Transactions on Software Engineering and Methodologies, Vol. 24, Num. 3, pages 1–42, 2015.

10. *Andrea Cerone*, Matthew Hennessy, Massimo Merro. *Modelling Mac-Layer Communications in Wireless Systems*. Logical Methods in Computer Science, Vol. 11, Num. 1, 2015.

11. *Gilles Barthe*. *High-Assurance Cryptography: Cryptographic Software We can Trust*. IEEE Security Privacy, Vol. 13, Num. 5, pages 86–89, 2015.

12. *Gilles Barthe*, Alberto Pardo, Gerardo Schneider. *SEFM: Software Engineering and Formal Methods*. Software and System Modeling, Vol. 14, Num. 1, pages 3–4, 2015.

13. Backes, Michael, *Boris Köpf*. *Quantifying information flow in cryptographic systems*. Mathematical Structures in Computer Science, Vol. 25, Num. 2, pages 457–479, 2015.

14. *Alejandro Sánchez*, *Cesar Sanchez*. *Parametrized Invariance for Infinite State Processes*. Acta Informatica, Vol. 52, Num. 6, pages 525–557, 2015.

15. Dario Catalano, *Dario Fiore*, Rosario Gennaro, Konstantinos Vamvourellis. *Algebraic*

(trapdoor) one-way functions: Constructions and applications. Theoretical Computer Science, Vol. 592, pages 143–165, Springer, 2015.

16. *Guillermo Vigueras*, Federico Sket, Cristóbal Samaniego, Ling Wu, Ludovic Noels, Denny Tjahjanto, Eva Casoni, Guillaume Houzeaux, Ahmed Makradi, Jon M. Molina-Aldareguia, Mariano Vázquez, Antoine Jérusalem. *An XFEM/CZM implementation for massively parallel simulations of composites fracture*. Composite Structures, Vol. 125, Num. 0, pages 542–557, 2015.

17. *Guillermo Vigueras*, Orduña, Juan M.. *On the Use of GPU for Accelerating Communication-Aware Mapping Techniques*. The Computer Journal, May 2015.

18. *Pavithra Prabhakar*, Geir E. Dullerud, Mahesh Viswanathan. *Stability Preserving Simulations and Bisimulations for Hybrid Systems*. IEEE Trans. Automat. Contr., Vol. 60, Num. 12, pages 3210–3225, 2015.

19. *Pavithra Prabhakar*, *Miriam García*. *AVERIST: An Algorithmic Verifier for Stability*. Electr. Notes Theor. Comput. Sci., Vol. 317, pages 133–139, 2015.

20. *Pavithra Prabhakar*, Parasara Sridhar Duggirala, Sayan Mitra, Mahesh Viswanathan. *Hybrid automata-based CEGAR for rectangular hybrid systems*. Formal Methods in System Design, Vol. 46, Num. 2, pages 105–134, 2015.

21. *Pavithra Prabhakar*, Vladimeros Vladimerou, Mahesh Viswanathan, Geir E. Dullerud. *A decidable class of planar linear hybrid systems*. Theoretical Computer Science, Vol. 574, pages 1–17, 2015.

22. Mila Dalla Preda, *Roberto Giacobazzi*, Saumya K. Debray. *Unveiling metamorphism by abstract interpretation of code properties*. Theor. Comput. Sci., Vol. 577, pages 74–97, 2015.

23. Isabella Mastroeni, *Roberto Giacobazzi*. *Weakening Additivity in Adjoining Closures*. Order, 2015.

Conferences

1. Shauvik Roy Choudhary, *Alessandra Gorla*, Alessandro Orso. *Automated Test Input Generation for Android: Are We There Yet?* Proceedings of the 30th IEEE/ACM International Conference on Automated Software Engineering, ASE 2015, pages 429–440, November 2015.

2. Irfan Ul Haq, *Juan Caballero*, Michael D. Ernst. *Ayudante: Identifying Undesired Variable Interactions*. Proceedings of the 13th International Workshop on Dynamic Analysis, October 2015.

3. Platon Kotzias, Srdjan Matic, Richard Rivera, *Juan Caballero*. *Certified PUP: Abuse in Authenticode Code Signing*. Proceedings of the 22nd ACM Conference on Computer and Communication Security, October 2015.

4. Srdjan Matic, Platon Kotzias, *Juan Caballero*. *CARONTE: Detecting Location Leaks for Deanonymizing Tor Hidden Services*. Proceedings of the 22nd ACM Conference on Computer and Communication Security, October 2015.

5. Salvador Tamarit, *Guillermo Vigueras*, *Manuel Carro*, Julio Mariño. *A Haskell Implementation of a Rule-Based Program Transformation for C Programs*. International Symposium on Practical Aspects of Declarative Languages, LNCS, Num. 9131, pages 105–114, Springer-Verlag, June 2015.

6. Vitalii Avdiienko, Konstantin Kuznetsov, *Alessandra Gorla*, Andreas Zeller, Steven Arzt, Siegfried Rasthofer, Eric Bodden. *Mining Apps for Abnormal Usage of Sensitive Data*. Proceedings of the 37th International Conference on Software Engineering, ICSE 2015, pages 426–436, ACM, May 2015.

7. Kurt Thomas, Elie Bursztein, Nav Jagpal, Moheeb Abu, Niels Provos, Paul Pearce, Grant Hoand Damon McCoy, Chris Grier, Vern Paxson, *Antonio Nappa*, Alexandros Kapravelos. *Ad*

Injection at Scale: Assessing Deceptive Advertisement Modifications. Proceedings of the 36th IEEE Symposium on Security and Privacy, pages 151–167, IEEE Computer Society, May 2015.

8. *Antonio Nappa*, Richard Johnson, Leyla Bilge, *Juan Caballero*, Tudor Dimitras. *The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching*. Proceedings of the 36th IEEE Symposium on Security and Privacy, May 2015.

9. *Ilya Sergey*, *Aleks Nanevski*, *Anindya Banerjee*. *Mechanized Verification of Fine-grained Concurrent Programs*. Proc. of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2015), pages 77–87, ACM, 2015.

10. *Ilya Sergey*, *Aleks Nanevski*, *Anindya Banerjee*. *Specifying and Verifying Concurrent Algorithms with Histories and Subjectivity*. Proc. of the 24th European Symposium on Programming (ESOP 2015), LNCS, pages 333–358, Springer, 2015.

11. Andrea Mattavelli, Alberto Goffi, *Alessandra Gorla*. *Synthesis of Equivalent Method Calls in Guava*. Proceedings of the 7th International Symposium on Search-Based Software Engineering, SSBSE 2015, pages 248–254, Springer, 2015.

12. *Andrea Cerone*, *Alexey Gotsman*, Hongseok Yang. *Transaction chopping for parallel snapshot isolation*. DISC'15: International Symposium on Distributed Computing, Tokyo, Japan, LNCS, Vol. 9363, pages 388–404, Springer, 2015.

13. *Andrea Cerone*, *Giovanni Bernardi*, *Alexey Gotsman*. *A framework for transactional consistency models with atomic visibility*. CONCUR'15: International Conference on Concurrency Theory, Madrid, Spain, LIPICS, Vol. 42, pages 58–71, Dagstuhl, 2015.

14. *Alexey Gotsman*, Hongseok Yang. *Composite replicated data types*. ESOP'15: European Symposium on Programming, London, UK, LNCS, Vol. 9032, pages 585–609, Springer, 2015.

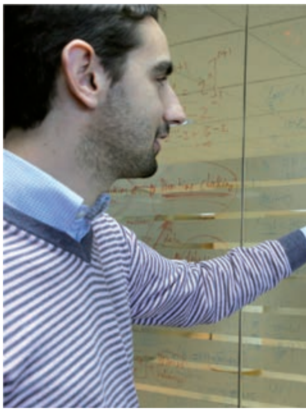
15. *Gilles Barthe*, Benjamin Grégoire, *Benedikt Schmidt*. *Automated Proofs of Pairing-based Cryptography*. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 1156–1168, ACM, 2015.

16. *Gilles Barthe*, Sonia Belaïd, *François Dupressoir*, Pierre-Alain Fouque, Benjamin Grégoire, *Pierre-Yves Strub*. *Verified Proofs of Higher-Order Masking*. Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 9056, pages 457–485, Springer, 2015.

17. *Gilles Barthe*, *Juan Manuel Crespo*, Yassine Lakhnech, *Benedikt Schmidt. Mind the Gap: Modular Machine-checked Proofs of One-round Key Exchange Protocols*. Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lecture Notes in Computer Science, Vol. 9057, pages 689–718, Springer, 2015.

18. Patrick Baillot, *Gilles Barthe*, Ugo Dal Lago. *Implicit Computational Complexity of Subrecursive Definitions and Applications to Cryptographic Proofs*. Logic for Programming, Artificial Intelligence, and Reasoning - 20th International Conference, LPAR-20 2015, Suva, Fiji, November 24-28, 2015, Proceedings, Lecture Notes in Computer Science, Vol. 9450, pages 203–218, Springer, 2015.

19. *Gilles Barthe*, Thomas Espitau, Benjamin Grégoire, Justin Hsu, Léo Stefanesco, *Pierre-Yves Strub*. *Relational Reasoning via Probabilistic Coupling*. Logic for Programming, Artificial Intelligence, and Reasoning - 20th International Conference, LPAR-20 2015, Suva, Fiji, November 24-28, 2015, Proceedings, Lecture Notes in Computer Science, Vol. 9450, pages 387–401, Springer, 2015.



20. *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*. Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2015, Mumbai, India, January 15-17, 2015, pages 55–68, ACM, 2015.

21. *Gilles Barthe*, Edvard Fagerholm, *Dario Fiore*, Andre Scedrov, *Benedikt Schmidt*, Mehdi Tibouchi. *Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds*. PKC 2015: 18th International Workshop on Theory and Practice in Public Key Cryptography, Lecture Notes in Computer Science, Vol. 9020, pages 355–376, Springer, 2015.

22. *Boris Köpf*. *Reasoning about the Trade-off between Security and Performance*. Proc. 12th International Conference on Quantitative Evaluation of Systems (QEST '15), Springer, 2015.

23. Klaus von Gleissenthall, *Boris Köpf*, Andrey Rybalchenko. *Symbolic Polytopes for Quantitative Interpolation and Verification*. Proc. 27th International Conference on Computer Aided Verification (CAV '15), Springer, 2015.

24. *Goran Doychev*, *Boris Köpf*. *Rational Protection Against Timing Attacks*. Proc. 28th IEEE Computer Security Foundations Symposium (CSF'15), IEEE, 2015.

25. Bernd Finkbeiner, Markus N. Rabe, *César Sánchez*. *Algorithms for Model Checking HyperLTL and HyperCTL**. Proc. of the 27th Int'l Conf. on Computer Aided Verification (CAV'15), LNCS, Vol. 9206, pages 30–48, Springer, 2015.

26. *Zorana Bankovic*, *Umer Liqat*, *Pedro Lopez-Garcia*. *A Practical Approach for Energy Efficient Scheduling in Multicore Environments by combining Evolutionary and YDS Algorithms with Faster Energy Estimation*. The 11th International Conference on Artificial Intelligence Applications and Innovations (AIAI'15), IFIP Advances in Information and Communication Technology, Vol. 458, pages 478–493, Springer, 2015.

27. *Zorana Bankovic*, *Umer Liqat*, *Pedro Lopez-Garcia*. *Trading-off Accuracy vs. Energy in Multicore Processors via Evolutionary Algorithms Combining Loop Perforation and Static Analysis-based Scheduling*. Hybrid Artificial Intelligent Systems (HAIS 2015), Lecture Notes in Computer Science, Vol. 9121, pages 690–701, Springer International Publishing, 2015.

28. *Zorana Bankovic*, *Pedro Lopez-Garcia*. *Improved Energy-aware Stochastic Scheduling based on Evolutionary Algorithms via Copula-based Modeling of Task Dependences*. International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2015), Advances in Intelligent Systems and Computing, Vol. 368, pages 153–163, Springer International Publishing, 2015.

29. *Zorana Bankovic*, *Pedro Lopez-Garcia*. *Energy Efficient Allocation and Scheduling for DVFS-enabled Multicore Environments using a Multiobjective Evolutionary Algorithm*. Genetic and Evolutionary Computation Conference (GECCO 2015), pages 1353–1354, ACM, 2015.

30. *José Francisco Morales*, *Manuel Hermenegildo*. *Pre-Indexed Terms for Prolog*. Proceedings of the 24th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'14), LNCS, Vol. 8981, pages 317–331, Springer, 2015.

31. Dario Catalano, *Dario Fiore*. *Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data*. ACM CCS 2015 – 22nd ACM Conference on Computer and Communication Security, pages 1518–1529, 2015.

32. Dario Catalano, *Dario Fiore*, *Luca Nizzardo*. *Programmable Hash Functions go Private: Constructions and Application to (Homomorphic) Signatures with Shorter Public Keys*. Advances

in Cryptology – CRYPTO 2015 – 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II, LNCS, Vol. 9216, pages 254–274, Springer, 2015.

33. Michael Backes, Manuel Barbosa, *Dario Fiore*, Raphael M. Reischuk. *ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data*. 36th IEEE Symposium on Security and Privacy (Oakland) 2015, IEEE Computer Society, 2015.

34. Antoine Jerusalem, *Guillermo Vigueras*, Federico Sket, Cristobal Samaniego, Ling Wu, Ludovic Noels, Denny Tjahjanto, Eva Casoni, Guillaume Houzeaux, Ahmed Makradi, Jon M. Molina-Aldareguia, Mariano Vazquez. *An XFEM/CZM implementation for massively parallel simulations of composites fracture*. European Solid Mechanics Conference, ESMC 2015, 2015.

35. Bishoksan Kafle, *John P. Gallagher*. *Tree automata-based refinement with application to Horn clause verification*. Verification, Model Checking, and Abstract Interpretation - 16th International Conference, VMCAI 2015, Mumbai, India, January 12-14, 2015. Proceedings, Lecture Notes in Computer Science, Vol. 8931, pages 209–226, Springer, 2015.

36. Bishoksan Kafle, *John P. Gallagher*. *Constraint Specialisation in Horn Clause Verification*. Proceedings of the 2015 Workshop on Partial Evaluation and Program Manipulation, PEPM, Mumbai, India, January 15-17, 2015, pages 85–90, Association for Computing Machinery, 2015.

37. Ahmed Bouajjani, *Michael Emmi*, Constantin Enea, Jad Hamza. *On Reducing Linearizability to State Reachability*. Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part II, pages 95–107, 2015.

38. *Michael Emmi*, Constantin Enea, Jad Hamza. *Monitoring Refinement via Symbolic Reasoning*. Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2015, Portland, OR, USA, June 15-17, 2015, pages 260–269, ACM, 2015.

39. Arvind Haran, Montgomery Carter, *Michael Emmi*, Akash Lal, Shaz Qadeer, Zvonimir Rakamaric. *SMACK+Corral: A Modular Verifier - (Competition Contribution)*. Tools and Algorithms for the Construction and Analysis of Systems - 21st International Conference, TACAS 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings, pages 451–454, 2015.

40. *Michael Emmi*, *Pierre Ganty*, Rupak Majumdar, Fernando Rosa-Velardo. *Analysis of Asynchronous Programs with Event-Based Synchronization*. Programming Languages and Systems - 24th European Symposium on Programming, ESOP 2015, Held as Part of the European Joint

Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings, pages 535–559, 2015.

41. Ahmed Bouajjani, *Michael Emmi*, Constantin Enea, Jad Hamza. *Tractable Refinement Checking for Concurrent Objects*. Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2015, Mumbai, India, January 15-17, 2015, pages 651–662, ACM, 2015.

42. *Carolina Inés Dania*, *Manuel Clavel*. *Model-Based Formal Reasoning about Data-Management Applications*. Fundamental Approaches to Software Engineering - 18th International Conference, FASE 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings, Lecture Notes in Computer Science, Vol. 9033, pages 218–232, Springer, 2015.

43. *Miguel Ángel García de Dios*, *Carolina Inés Dania*, *Manuel Clavel*. *Formal Reasoning about Fine-Grained Access Control Policies*. 11th Asia-Pacific Conference on Conceptual Modelling, APCCM 2015, Sydney, Australia, January 2015, CRPIT, Vol. 165, pages 91–100, Australian Computer Society, 2015.

44. *Pavithra Prabhakar*, Nima Roohi, Mahesh Viswanathan. *Deciding Concurrent Planar Monotonic Linear Hybrid Systems*. Formal Modeling and Analysis of Timed Systems - 13th International Conference, FORMATS 2015, Madrid, Spain, September 2-4, 2015, Proceedings, pages 256–269, 2015.

45. *Pavithra Prabhakar*, *Miriam García*. *Foundations of Quantitative Predicate Abstraction for Stability Analysis of Hybrid Systems*. Verification, Model Checking, and Abstract Interpretation - 16th International Conference, VMCAI 2015, Mumbai, India, January 12-14, 2015. Proceedings, Lecture Notes in Computer Science, Vol. 8931, pages 318–335, Springer, 2015.

46. *Pierre Ganty*, Samir Genaim, Ratan Lal, *Pavithra Prabhakar*. *From Non-Zenoness Verification to Termination*. MEMOCODE '15: 13th ACM-IEEE Int. Conf. on Formal Methods and Models for System Design, IEEE Computer Society, 2015.

47. Javier Esparza, *Pierre Ganty*, Jérôme Leroux, Rupak Majumdar. *Verification of Population Protocols*. CONCUR '15: Proc. 26th Int. Conf. on Concurrency Theory, 2015.

48. Antoine Durand-Gasselin, Javier Esparza, *Pierre Ganty*, Rupak Majumdar. *Model Checking Parameterized Asynchronous Shared-Memory Systems*. CAV '15: Proc. 25th Int. Conf. on Computer Aided Verification, LNCS, Vol. 9206, Springer, 2015.

49. *Pierre Ganty*, Radu Iosif. *Interprocedural Reachability for Flat Integer Programs*. FCT '15: Proc. 20th Int. Symp. on Fundamentals of Computation Theory, LNCS, Springer, 2015.

50. Ratan Lal, *Pavithra Prabhakar*. *Bounded error flowpipe computation of parameterized linear systems*. Proceedings of the International Conference on Embedded Software (EMSOFT), ACM, IEEE, 2015.

51. *Roberto Giacobazzi*, Francesco Logozzo, Francesco Ranzato. *Analyzing Program Analyses*. Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2015, Mumbai, India, January 15-17, 2015, pages 261–273, 2015.

52. Mila Dalla Preda, *Roberto Giacobazzi*, Arun Lakhotia, Isabella Mastroeni. *Abstract Symbolic Automata: Mixed syntactic/semantic similarity analysis of executables*. Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2015, Mumbai, India, January 15-17, 2015, pages 329–341, 2015.

Workshops

1. Bishoksan Kafle, *John P. Gallagher*, *Pierre Ganty*. *Decomposition by tree dimension in Horn clause verification*. 3rd Int. Workshop on Verification and Program Transformation (VPT '15), EPTCS 199, 2015, pages 1-14, arXiv:1512.03862.

2. S. Gurses, *Carmela Troncoso*, C. Diaz. *Engineering Privacy by Design Reloaded*. Privacy Conference, Amsterdam, 2015.

3. *Joaquín Arias Herrero*, *Manuel Carro*. *Towards a Generic Interface to Integrate CLP and Tabled Execution (Extended Abstract)*. Proceedings of the Technical Communications of the 31st International Conference on Logic Programming (ICLP 2015), Cork, Ireland, August 31 - September 4, 2015, CEUR Workshop Proceedings, Vol. 1433, CEUR-WS.org, 2015. Extended Abstract.

4. *Pedro Lopez-Garcia*, *Remy Haemmerle*, *Maximiliano Klemen*, *Umer Liqat*, *Manuel Hermenegildo*. *Towards Energy Consumption Verification via Static Analysis*. Workshop on High Performance Energy Efficient Embedded Systems (HIP3ES), arXiv:1501.03064, 2015. arXiv:1512.09369.

6.1.2. Articles in Books and other Collections

1. *Gilles Barthe*, François Dupressoir, Benjamin Grégoire, *Benedikt Schmidt*, *Pierre-Yves Strub*. *Computer-Aided Proofs in Cryptography: An Overview*. All about Proofs, Proofs for All (APPA), Mathematical Logic and Foundations, Vol. 55, College Publications, January 2015.

2. Konstantin Kuznetsov, *Alessandra Gorla*, Ilaria Tavecchia, Florian Gross, Andreas Zeller. *Mining Android Apps for Anomalies*. The Art and Science of Analyzing Software Data, pages 257–284, Morgan Kaufmann, 2015.

6.1.3. Edited Volumes

1. *Gilles Barthe*, Andrew D. Gordon, Joost-Pieter Katoen, Annabelle McIver. *Challenges and Trends in Probabilistic Programming (Dagstuhl Seminar 15181)*. Dagstuhl Reports, Vol. 5, Num. 4, pages 123–141, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.

2. Frank Piessens, *Juan Caballero*, Nataliia Bielova. *Engineering Secure Software and Systems - 7th International Symposium, ESSoS 2015, Milan, Italy, March, 4-6, 2015. Proceedings*. Lecture Notes in Computer Science, Vol. 8978, Springer, 2015.

6.1.4. Doctoral, Master and Bachelor Theses

1. Miguel A. García de Dios. *Model-driven Development of Secure Data-Management Applications*. PhD Thesis. Universidad Complutense de Madrid (UCM). April 2015. Advisor: Manuel Clavel (IMDEA Software Institute).

2. Alejandro Sánchez. *Formal Verification of Temporal Properties for Parametrized Concurrrent Programs and Concurrent Data Structures*. PhD Thesis. Technical University of Madrid (UPM). September 2015. Advisor: César Sánchez (IMDEA Software Institute).

3. Tahir Javaid Cheema. *Testing of Android Testing Tools: Development of a Benchmark for the Evaluation*. MSc Thesis. Technical University of Madrid (UPM). July 2015. Advisor: Alessandra Gorla (IMDEA Software Institute).

4. Maximiliano Klemen. *Improved Static Analysis and Verification of Energy Consumption and other Resources via Abstract Interpretation*. MSc Thesis. Technical University of Madrid (UPM). July 2015. Advisor: Pedro Lopez-Garcia (IMDEA Software Institute).

5. Joaquín Arias. *Design and implementation of a modular interface to integrate CLP and tabled execution*. MSc Thesis. Technical University of Madrid (UPM). July 2015. Advisor: Manuel Carro (IMDEA Software Institute).

6. Guillermo Ramos. *Implementing a Term Rewriting Engine for the EasyCrypt Framework*. MSc Thesis. Technical University of Madrid (UPM). July 2015. Advisor: Pierre-Yves Strub (IMDEA Software Institute).

7. Marcos Sebastián Alarcón. *Design and Implementation of an Endpoint Reputation Module*. BSc Thesis. Technical University of Madrid (UPM). January 2015. Advisor: Juan Caballero (IMDEA Software Institute).

8. Rosario Sebastiano Russo. *A Framework for Implementing Outsourcing Schemes*. MSc Thesis. Technical University of Madrid (UPM). July 2015. Advisor: Dario Fiore (IMDEA Software Institute).

6.2. Invited Talks

6.2.1. Invited and Plenary Talks by IMDEA Scientists

1. *Gilles Barthe*. Computer-Aided Cryptography. Invited talk at the 21st Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2015). Auckland, New Zealand. December 2015.

2. *Gilles Barthe*. Towards high-assurance cryptographic implementations. Invited talk at the 14th International Conference on Cryptology and Network Security (CANS 2015). Le Meridien N'Fis, Marrakesh, Morocco. December 2015.

3. *Gilles Barthe*. Towards Verified Cryptographic Implementations. Invited talk at the 25th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2015). Siena, Italy. July 2015.

4. *Gilles Barthe*. Computer-Aided Cryptography. Invited talk at the 21st International Conference on Types for Proofs and Programs (TYPES 2015). Tallin, Estonia. May 2015.

5. *Juan Caballero*. Invited panel on "Cybersecurity" at the 26th European Regional International Telecommunication Society Conference, San Lorenzo del Escorial, Spain. June 2015.

6. *Juan Caballero*. Invited panel on "European Entrepreneurs in digital innovation and education" at Spain Startup South Summit, Madrid, Spain. October 2015.

7. *Manuel Carro*. Formal Methods in Industry. Valencia, May 2015.

8. *Manuel Carro*. Rule-Based Program Transformation for Hybrid Architectures. Invited talk at the Hybrid Systems workshop, Computing Systems Week. Oslo, May 2015.

9. *Manuel Carro*. The IMDEA Software Institute. Invited talk at the series on "Success formulas in research management in Spain". Santiago de Compostela, June 2015.

10. *Manuel Clavel*. Model-Based Formal Analysis of Data-Management Applications. Invited talk at the International Conference on Advanced Computing and Applications (ACOMP 2015). Ho Chi Minh City, Vietnam. November 2015.

11. *François Dupressoir*. Computer-Aided Cryptographic Proofs for Low-Level Implementations. Invited talk at the Workshop on Implementation: Security and Evaluation (WISE), Paris, France. September 2015.

12. *Dario Fiore*. Ensuring integrity in Cloud computing via homomorphic digital signatures: new tools and results. Invited talk at CyberCamp 2015, Madrid, Spain. November 2015.

13. *Pierre Ganty*. Parameterized Verification of Asynchronous Shared-Memory Systems. Invited talk at the ACTS 2015 Workshop, Chennai Mathematical Institute, India. February 2015.

14. *Roberto Giacobazzi*. Obscuring Code – Unveiling and Veiling Information in Programs. Invited keynote at Jornadas sobre PROgramación y LEnguajes (PROLE 2015), Santander, Spain. September 2015.

15. *Roberto Giacobazzi*. Obscuring Code – Unveiling and Veiling Information in Programs. Merit Invited lecture, University of Melbourne, Melbourne, Australia. May 2015.

16. *Alessandra Gorla*. Towards using Android testing tools to assess trustworthiness of apps. Keynote talk at TESTBEDS workshop, Lincoln, Nebraska, USA. November 2015.

17. *Alessandra Gorla*. Advances and current challenges in mining anomalies. Keynote at Workshop in Recent Advances in Secure Software Engineering. September 2015.

18. *Alexey Gotsman*. Analysing and Optimising Parallel Snapshot Isolation. Invited talk at the UPMARC Workshop on Memory Models, Uppsala, Sweden. February 2015.

19. *Boris Koepf*. Reasoning about the Trade-off between Security and Performance. Invited keynote at 12th International Conference on Quantitative Evaluation of Systems (QEST 2015). Madrid, Spain. September 2015.

20. *Aleks Nanevski*. Dependent Types for Specification and Verification of Concurrent Programs. Invited keynote at the 31st Conference on the Mathematical Foundations of Programming Semantics. Nijmegen, Netherlands. June 2015.

21. *Carmela Troncoso*. Privacy-preserving Smart City: utopia or reality? Invited talk at the Panel at Smart City Expo World Congress. Barcelona, Spain. November 2015.

6.2.2. Invited Seminars and Lectures by IMDEA Scientists

1. *Anindya Banerjee*. Modular Reasoning for Behavior-Preserving Data Structure Refactorings. Invited talk at Indiana University, Bloomington, USA. February 2015.

2. *Anindya Banerjee*. Modular Reasoning for Behavior-Preserving Data Structure Refactorings. Invited talk at Tel Aviv University, Tel Aviv, Israel. May 2015.

3. *Anindya Banerjee*. Modular Reasoning for Behavior-Preserving Data Structure Refactorings. Invited talk at MFCS 2015, Milano, Italy. August 2015.

4. *Giovanni Bernardi*. Using higher-order contracts to model session types. Invited talk at University Paris Diderot, France. May 2015.

5. *Giovanni Bernardi*. Using higher-order contracts to model session types. Invited talk at University of Genova, Italy. August 2015.

6. *Giovanni Bernardi*. Using higher-order contracts to model session types. Invited talk at INRIA Rhone Alpes, France. November 2015.

7. *Juan Caballero*. Internet-Wide Scanning and its Security Applications. Invited talk at MC2 Workshop, University of Maryland at College Park, USA. January 2015.

8. *Juan Caballero*. CyberProbe & AutoProbe: Towards Internet-Scale Active Detection of Malicious Servers. Invited talk at Università di Trento, Italy. April 2015.

9. *Juan Caballero*. CyberProbe & AutoProbe: Towards Internet-Scale Active Detection of Malicious Servers. Invited talk at University of Texas in Dallas, USA. May 2015.

10. *Juan Caballero*. Malware, Cibercrimen y Técnicas Activas de Detección de Infraestructuras Maliciosas. Invited seminar at Escuela de Verano en Diseño Seguro y Análisis de Sistemas. Universidad de León, Spain. July 2015.

11. *Juan Caballero*. Caronte: Detecting Location Leaks for Deanonymizing Tor Hidden Services. Invited talk on at TrendMicro FTR meeting, Madrid, Spain. September 2015.

12. *Juan Caballero*. CyberProbe & AutoProbe: Towards Internet-Scale Active Detection of Malicious Servers. Invited talk at Eurecom, Sophia-Antipolis, France. September 2015.

13. *Andrea Cerone*. Formalising and Optimising Parallel Snapshot Isolation. Invited talk at IMT Lucca, Italy. January 2015.

14. *Andrea Cerone*. Analysing and Optimising Parallel Snapshot Isolation. Invited talk at Schloss Dagstuhl. May 2015.

15. *Goran Doychev*. Rational Protection Against Timing Attacks. Invited talk at TU Berlin, Germany. September 2015.

16. *François Dupressoir*. Computer-Aided Cryptographic Proofs for Low-Level Implementations. Invited talk at the Seminar on Formal Methods and Security, INRIA Rennes, France. July 2015.

17. *François Dupressoir*. Computer-Aided Cryptographic Proofs for Low-Level Implementations. IACR School on Computer-Aided Cryptography. University of Maryland, College Park, USA. June 2015.

18. *François Dupressoir*. Towards Provably-Secure Optimizing Masking Compilers. Invited talk at the Real-World Cryptography Workshop (RWC 2015), London, UK. January 2015.

19. *Dario Fiore*. Advanced Cryptographic Techniques for Secure Outsourcing to the Cloud. Invited lecture at Universidad Carlos III, Madrid, Spain. February 2015.

20. *Dario Fiore*. Boosting Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data. École Normale Supérieure, Paris, France. March 2015.

21. *Dario Fiore*. Efficiently Verifiable Computation on Encrypted Data. CryptoAction WG1 meeting, Warsaw, Poland. March 2015.

22. *Dario Fiore*. Asymmetric Programmable Hash Functions and Applications to (Homomorphic) Signatures with Short Public Keys. Workshop in Cryptography, Bochum. April 2015.

23. *Dario Fiore*. Boosting Linearly-Homomorphic Encryption. Invited lecture at Congreso de Jovenes Investigadores, RSME, Murcia, Spain. September 2015.

24. *Dario Fiore*. Programmable Hash Functions go Private: Constructions and Applications to (Homomorphic) Signatures with Short Public Keys. Cryptography Seminars Day at UPC, Barcelona, Spain. September 2015.

25. *John Gallagher*. Invited tutorial on analysis and verification of imperative programs through CLP. 31st International Conference on Logic Programming (ICLP 2015). Cork, Ireland. September 2015.

26. *Roberto Giacobazzi*. Abstract Non-Interference. Invited talk at the Shonan Meeting on Logic and Verification Methods in Security and Privacy. Tokyo Shonan Village Center, Tokyo Japan. October 2015.

27. *Roberto Giacobazzi*. Analysis for Trustworthy apps on untrusted platforms. Irdeto, Ottawa, Canada. July 2015.

28. *Roberto Giacobazzi*. Abstract Symbolic Automata. Invited talk at the Shonan Meeting on Low level code analysis and applications to computer security. Tokyo Shonan Village Center, Tokyo Japan. March 2015.

29. *Roberto Giacobazzi*. Completeness in Abstract Interpretation. University of Melbourne, Melbourne, Australia. May 2015.

30. *Roberto Giacobazzi*. Big Code and software security. University of Verona, Verona, Italy. March 2015.

31. *Alessandra Gorla*. Challenges and Opportunities in Mobile Testing. Invited course at the 11th International Summer School on Training And Research On Testing, Cadiz, Spain. June 2015.

32. *Alessandra Gorla*. Mining behavior of Android apps: Can test input generation tools help? Invited talk at Shonan meeting on Mobile App Store Analytics. October 2015.

33. *Alexey Gotsman*. Reasoning about consistency choices in distributed systems. Amazon Web Services, Herndon, VA, USA. June 2015.

34. *Alexey Gotsman*. Reasoning about consistency choices in distributed systems. Technion University, Israel. August 2015.

35. *Alexey Gotsman*. Analysing and Optimising Parallel Snapshot Isolation. University of Oxford, UK. March 2015.

36. *Boris Koepf*. Rational Protection Against Timing Attacks. Invited talk at CISPA, Saarland University. April 2015.

37. *Boris Koepf*. The Economics of Side Channel Attacks. Invited talk at NSF Workshop on Formal Methods for Information Security. College Park, USA. November 2015.

38. *Boris Koepf*. Rational Protection Against Timing Attacks. Invited talk Dagstuhl Seminar Challenges and Trends in Probabilistic Programming. April 2015.

39. *Umer Liqat*. Recent Developments in the CiaoPP Resource Analysis Tools. ENTRA Workshop, Malaga, Spain. May 2015.

40. *Antonio Nappa*. Active Detection Technique of Malicious Infrastructures. Invited talk at University of Saarland, Germany. November 2015.

41. *Ilya Sergey*. Programming with Proofs. Invited talk at Google, London, UK. April 2015.

42. *Ilya Sergey*. Programming and Proving with Concurrent Resources. Invited talk at University College London, UK. April 2015.

43. *Pierre-Yves Strub*. An introduction to Provable Security using the EasyCrypt Proof Assistant. Invited talk at CEA LIST. Saclay, France.

6.2.3. Invited Speaker Series

During 2015, 21 external speakers were invited to give talks at IMDEA Software. All of our seminars and talks are open to the campus and the academic community at large. The following list shows the speakers and the titles of their talks.

1. *Juan P. Galeotti*. Post-doctoral Researcher, Saarland University, Germany: Automated test generation for classes with environment dependencies.

2. *Ben Livshits*. Research Scientist, Microsoft Research: Program Boosting: Program Synthesis via Crowd-Sourcing.

3. *Markku Oivo*. Professor, University of Oulu, Finland: Overview of working lines of the M-GROUP (Department of Information Processing Science, University of Oulu, FI).

4. *Beta Ziliani*. PhD Student, Max Planck Institute for Software Systems, Saarbruecken, Germany: A Predictable Unification Algorithm for Coq Featuring Universe Polymorphism and Overloading.

5. *Ben Livshits*. Research Scientist, Microsoft Research: PrePose: Security and Privacy for Gesture-Based Programming.

6. *David Atienza*. Associate Professor, EPFL, Switzerland: Ultra-Low Power Design of Multimodal BioSignal Wearable Systems.

7. *Jose Manuel Fernandez de Labastida*. Head of Scientific Management Department, European Research Council: Funding opportunities in the European Research Council.

8. *Andreas Zeller*. Full Professor, Saarland University, Germany: Mining Sandboxes.

9. *Luis Maria Ferrer Fioriti*. PhD Student, Saarland University, Germany: Probabilistic termination.

10. *Alberto Goffi and Andrea Mattavelli*. PhD Students, Università della Svizzera Italiana, Lugano, Switzerland: Exploiting Intrinsic Redundancy to Automatically Generate Test Oracles.

11. *Cheng Li*. PhD Student, Max Planck Institute for Software Systems, Germany: Automating the Choice of Consistency Levels in Replicated Systems.

12. *Radu Iosif*. CNRS Researcher (CR1), Distributed and Complex Systems Group, VERIMAG/CNRS, Grenoble, France: Decidable Horn Systems with Difference Constraints Arithmetic.

13. *Sina Shamshiri*. PhD Student, University of Sheffield, UK: Random or Genetic Algorithm Search for Object-Oriented Test Suite Generation?

14. *Jose Miguel Rojas*. Research Associate, University of Sheffield, UK: Automated Unit Test Generation during Software Development: A Controlled Experiment and Think-Aloud Observations.

15. *Adam Chlipala*. Associate Professor, Languages & Verification Group, MIT, USA: Phantom Monitors: A Simple Foundation for Modular Proofs of Fine-Grained Concurrent Programs.

16. *Sriram Sankaranarayanan*. Professor, University of Colorado Boulder, USA: Invariants on expected values in probabilistic programs.

17. *Joost-Pieter Katoen*. Full Professor, RWTH Aachen, Germany: Understanding and Analyzing Probabilistic Programs.

18. *Klaus von Gleissenthall*. PhD Student, TU Munich, Germany: Synthesizing Cardinality Invariants for Parameterized Systems.

19. *Elena Pagnin*. PhD Student, Chalmers, Sweden: Attacks against Privacy-Preserving Biometric Authentication systems.

20. *Günes Acar*. PhD Student, KU Leuven, Belgium: Advanced Web Tracking Mechanisms.

21. *Sebastian Faust*. Assistant Professor, Ruhr-University of Bochum, Germany: Leakage Resilient Masking Schemes.

6.2.4. Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of **32** seminars were given in 2015.

6.3. Scientific Service and Other Activities

6.3.1. Conference and Program Committee Chairmanship

Juan Caballero:

1. TPC Co-chair of the 7th International Symposium on Engineering Secure Software and Systems (ESSoS 2015).

2. TPC Co-chair of the 8th European Workshop on Systems Security (EuroSec 2015).

Pierre Ganty

1. Program co-chair of the 10th International Symposium on Trustworthy Global Computing (TGC 2015).

Alessandra Gorla:

1. Tool Demonstrations co-chair, IEEE and ACM International Conference on Automated Software Engineering (ASE 2015).

Boris Koepf:

1. PC Co-chair of the Workshop on Foundations of Computer Security (FCS 2015).

6.3.2. 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 IEEE European Symposium on Security and Privacy (Euro S&P).

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

Manuel Carro:

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

Dario Fiore:

1. Editorial board of IET Information Security.

John Gallagher:

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

Roberto Giacobazzi:

1. Steering Committee of Symposium on Principles of Programming Languages (POPL).

2. Steering Committee of Static Analysis Symposium (SAS).

3. Scientific Advisory Board of the 6th International Summer School on Information Security and Protection.

Alexey Gotsman:

1. Steering committee of Workshop on Principles and Practice of Consistency for Distributed Data (PaPoC), affiliated with EuroSys.

Manuel Hermenegildo:

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

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

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

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

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

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

7. Area Editor, Algorithms in Programming Languages and Software Engineering, of the "Journal of the IGPL" (Oxford U press).

Boris Koepf:

1. Steering committee of IEEE Computer Security Foundations Symposium (CSF).

2. Steering committee of Workshop on Foundations of Computer Security (FCS).

Pablo Nogueira:

1. Steering Committee of the International Conference on Mathematics of Program Construction.

6.3.3. Participation in Program Committees

Zorana Bankovic:

1. 16th International Conference on Engineering Applications of Neural Networks (EANN 2015).

2. 11th International Conference on Artificial Intelligence Applications and Innovations (AIAI 2015).

Gilles Barthe:

1. 22nd ACM Conference on Computer and Communications Security (ACM CCS 2015).

2. 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2015).

3. Thirtieth Annual ACM/IEEE Symposium on Logic In Computer Science (LICS 2015).

4. 24th European Symposium on Programming (ESOP 2015).

5. 20th International Symposium on Formal Methods (FM 2015).

Juan Caballero:

1. 22nd ACM Conference on Computer and Communications Security (ACM CCS 2015).

2. I Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2015).

3. 9th USENIX Workshop on Offensive Technologies (WOOT 2015).

4. 24th USENIX Security Symposium (USENIX Security 2015).

5. 2015 Network and Distributed System Security Symposium (NDSS 2015).

Manuel Carro:

1. 31st International Conference on Logic Programming (ICLP 2015).

2. 17th International Conference on Service Oriented Computing (ICSOC 2015).

3. 8th IEEE International Conference on Service Oriented Computing & Applications, PhD Symposium (SOCA 2015).

4. XV Jornadas de PROgramación y LEnguajes (PROLE 2015).

Manuel Clavel:

1. 15th International Workshop on OCL and Textual Modeling Applications and Case Studies (OCL 2015).

2. ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (MODELS 2015).

Francois Dupressoir:

1. Workshop on Security Proofs for Embedded Systems (PROOFS 2015).

Dario Fiore:

1. International Workshop on Security in Cloud Computing (SCC 2015).

2. 3rd Workshop on Applied Homomorphic Cryptography and Encrypted Computing (WAHC 2015).

3. 18th International Conference on Practice and Theory in Public Key Cryptography (PKC 2015).

4. 35th International Cryptology Conference (CRYPTO 2015).

5. 22nd ACM Conference on Computer and Communications Security (ACM CCS 2015).

6. I Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2015).

John Gallagher:

1. Second Workshop on Horn Clauses for Verification and Synthesis (HCVS 2015).

2. Third International Workshop on Verification and Program Transformation (VPT 2015).

Pierre Ganty:

1. 6th International Symposium on Games, Automata, Logics and Formal Verification (GandALF 2015).

2. 17th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2015).

Roberto Giacobazzi:

1. 22nd International Static Analysis Symposium (SAS 2015).

2. 1st International Workshop on Software PROtection (SPRO 2015), in conjunction with ICSE 2015.

Alessandra Gorla:

1. 3rd International Workshop on Software Development Lifecycle for Mobile (DeMobile 2015).

2. 10th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2015) (Artifact Evaluation committee).

3. 30th IEEE and ACM International Conference on Automated Software Engineering (ASE 2015) (member of the Expert Review Panel).

4. ACM International Symposium on Software Testing and Analysis (ISSTA 2015).

5. 37th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2015), Software Engineering In Practice track.

6. 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS) 2015, co-located with the IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE).

7. Italian Student Contest on Software Engineering (SCORE-it) 2015, co-located with the IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE).

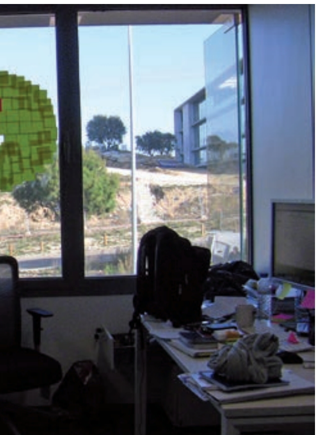
Alexey Gotsman:

1. Programming Language Approaches to Concurrency- and Communication-cEntric Software (PLACES 2015).

2. 15th International Conference on Application of Concurrency to System Design (ACSD 2015).

3. 13th Asian Symposium on Programming Languages and Systems (APLAS 2015).

4. 24th European Symposium on Programming (ESOP 2015).



Rémy Haemmerlé:

1. 24th International Joint Conference on Artificial Intelligence (IJCAI 2015).

Manuel Hermenegildo:

1. 6th workshop on Tools for Automatic Program Analysis (TAPAS 2015).

2. Foundational and Practical Aspects of Resource Analysis (FOPARA 2015).

3. 25th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2015).

Boris Koepf:

1. 28th IEEE Computer Security Foundations Symposium (CSF 2015).

2. 12th International Conference on Quantitative Evaluation of Systems (QEST 2015).

José Morales:

1. International Conference on Logic Programming (ICLP) Doctoral Consortium 2015.

Aleks Nanevski:

1. 21st International Conference on Types for Proofs and Programs, (TYPES 2015).

Pavithra Prabhakar:

1. 55th American Control Conference (ACC 2015).

2. 5th IFAC Conference on Analysis and Design of Hybrid Systems (IFAC ADHS 2015).

3. 16th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2015).

4. 8th International Workshop on Numerical Software Verification (NSV 2015).

5. 15th International Conference on Runtime Verification (RV 2015).

6. 18th ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2015).

Cesar Sanchez:

1. 13th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'15).

2. 6th IPM International Conference on Fundamentals of Software Engineering (FSEN'15).

3. 30th Annual ACM Symposium On Applied Computing (SAC) Track on Service-Oriented Architectures and Programming (SOAP 2015).

4. 9th International Symposium on Theoretical Aspects of Software Engineering (TASE 2015).

5. 2nd Workshop on formal verification for self-* systems (VERY* 2015).

Benedikt Schmidt:

1. Workshop on Foundations of Computer Security (FCS 2015).

Ilya Sergey:

1. International Workshop on Scripts to Programs (STOP 2015).

Carmela Troncoso:

1. International Conference on Financial Cryptography and Data Security 2015.

2. Selected Areas in Cryptography 2015.

6.3.4. Association and Organization Committees

Gilles Barthe:

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

2. Dagsthul seminar on Challenges and Trends in Probabilistic Programming.

Roberto Giacobazzi:

1. 6th International Summer School on Information Security and Protection. Rio de Janeiro, Brazil. July 2015.

Manuel Carro:

1. Representative of UPM in ERCIM.

2. Deputy representative of IMDEA Software in Informatics Europe.

3. Co-Location Manager and Scientific Coordinator of the EIT Digital Madrid Associate Partner Group.

Manuel Clavel:

1. 1st Workshop on Data Privacy Management and its Implementation in eHealth Systems, Ho Chi Minh City, Vietnam. February 2015.

Dario Fiore:

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

2. Co-organizer of the first Itinerant Cryptography Seminar. January 2015.

Manuel Hermenegildo:

1. Director, EIT Digital Madrid Associate Partner Group.

2. Elected member Informatics Europe executive board.

3. Vice-President of Informatics Europe. Member Informatics Europe department evaluation board.

4. Elected President of SpaRCIM.

5. Member *Academia Europaea*.

6. Member of Schloss Dagstuhl scientific advisory board.

7. Member IRILL (French Institute for Free Software) scientific board.

8. Secretary of the International Association for Logic Programming.

9. Member of the International Federation for Computational Logic (IFCoLog) Advisory OBoard.

Benedikt Schmidt:

1. Co-organizer of the IACR Summer School on Computer-Aided Cryptography, University of Maryland, College Park, USA, June 2015.

Carmela Troncoso:

1. Editorial Board Proceedings on Privacy Enhancing Technologies (PoPETs).

2. Steering Committee of Privacy Enhancing Technologies Symposium (PETS).

6.4. Awards

Conference Paper Awards:

1. Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cedric Fournet, Markulf Kohlweiss, Alfredo Pironti, *Pierre-Yves Strub*, Jean Karim Zinzindohoue. A Messy State of the Union: Taming the Composite State Machines of TLS. 2015 IEEE Symposium on Security & Privacy (Oakland 2015). **Distinguished paper award.**

2. Kurt Thomas, Elie Bursztein, Nav Jagpal, Moheeb Abu, Niels Provos, Paul Pearce, Grant Ho, Damon McCoy, Chris Grier, Vern Paxson, *Antonio Nappa*, Alexandros Kapravelos. Ad Injection at Scale: Assessing Deceptive Advertisement Modifications. 2015 IEEE Symposium on Security & Privacy (Oakland 2015). **Best practical paper award.**

3. Dario Catalano, *Dario Fiore*, *Luca Nizzardo*. Programmable Hash Functions go Private: Constructions and Applications to (Homomorphic) Signatures with Shorter Public Keys. I Jornadas Nacionales de Investigacion en Ciberseguridad (JNIC 2015). **Best paper award (category "Short papers").**

4. Bishoksan Kafle, *John P. Gallagher*. Constraint Specialisation in Horn Clause Verification. PEPM workshop 2015. **Best paper award.**

5. *Zorana Bankovic*, *Umer Liqat*, and *Pedro Lopez-Garcia*. A PracticalApproach for Energy Efficient Scheduling in Multicore Environments by combining Evolutionary and YDS Algorithms with Faster Energy Estimation. 11th International Conference on Artificial Intelligence Applications and Innovations (AIAI 2015). **Best paper award.**

Other Awards:

1. A. Haran, M. Carter, *M. Emmi,* A. Lal, S. Qadeer, and Z. Rakamaric. SMACK+Corral: A Modular Verifier. In Proc. 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2015). **SMACK+Corral, the tool described in that paper, was the winner of two gold medals, one silver medal, and one bronze medal at the 4th International Competition on Software Verification (SV-COMP 2015).**

6.5. Dissemination Events

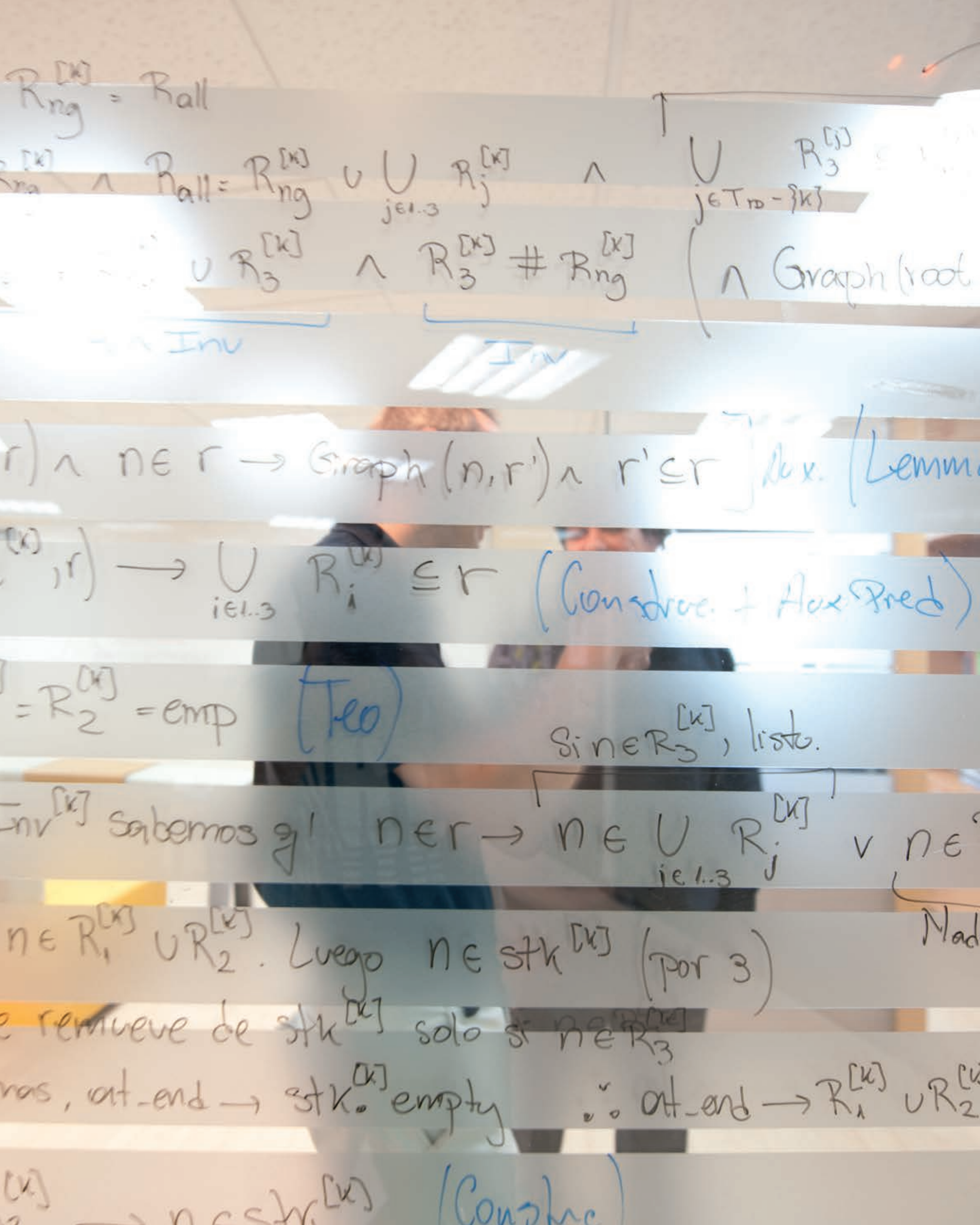
In 2015 IMDEA Software researchers have participated to a number of events related to dissemination and the promotion of science.

Researcher's Night. In September 2015, as in previous years, the IMDEA Software Institute participated in the European-wide initiative "Researchers' Night", which this year had as unifying topic "*Science and movie scientists: Does reality surpass fiction?*" Taking their field of expertise as starting point, researchers from the IMDEA Institutes showed the many facets of the film industry and science. To do so, following the layout of a live talk show, they spoke of the image of science and movie scientists, of the sciences that nurture the so-called seventh art... and, above all, of themselves: of what drove them to pursue their research, and if their character, drive and work are similar to what is shown in movies. The show was participated by IMDEA Software Institute researchers Manuel Hermenegildo (director) and Manuel Carro (deputy director).

Full description:
http://www.imdea.org/events/imdea-initiative/2015/science-movie-scientists-does-reality-surpass-fiction

Industrial and Entrepreneurship-Oriented Events. The IMDEA Software Institute is strongly committed to supporting technology transfer and collaboration with industry. In addition to all the forms of transfer and collaboration mentioned before (from research projects with industrial partners committed to the commercial exploitation of results to all the activities of the Spanish associate node of EIT Digital, significant accelerators of such transfer), important additional missions are to disseminate results and to create awareness of the return on investment of research. To this end, the Institute organizes and participates in a wide range of industrial and entrepreneurship-oriented events, which in 2015 included the following:

1. EIT Digital *Transfiere* (Malaga). February 2015.
2. EIT INNOVEIT. May 2015.
3. EIT/UPM: Data Science Master Welcome Day. September 2015.
4. EIT FI-PPP Liaison Demo / info day. September 2015.
5. EIT: Spain Startup / South Summit. October 2015.
6. EIT Digital *Raising I&E Awareness*. November–December 2015.
7. Innovatech Industrial Workshops, with UPM. December 2015.


$R_{ng}^{[k]} = R_{all}$
$R_{all} = R_{ng}^{[k]} \cup \bigcup_{j \in 1..3} R_j^{[k]} \wedge \bigcup_{j \in T_{rp} - \{k\}} R_3^{[j]}$
$\cup R_3^{[k]} \wedge R_3^{[k]} \# R_{ng}^{[k]}$ ($\wedge$ Graph(root
Inv
Inv
$r) \wedge n \in r \rightarrow$ Graph$(n, r') \wedge r' \subseteq r$] Aux. (Lemm
$,r) \longrightarrow \bigcup_{i \in 1..3} R_i^{[k]} \subseteq r$ (Consdrac. + Aux 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 $n \in R_3^{[k]}$
mos, at_end $\rightarrow stk^{[k]}$ empty $\therefore$ at_end $\rightarrow R_1^{[k]} \cup R_2^{[k]}$
$\rightarrow n \in stk^{[k]}$ (Consdrac

scientific highlights

7

the freak at

The FREAK Attack

IMDEA Software Institute researchers, together with colleagues at INRIA Rocquencourt, France and Microsoft Research Cambridge, UK uncovered a vulnerability in a popular encryption mechanism, known as TLS, that is used widely on the Internet to access web pages securely. The flaw, dubbed "FREAK: Factoring RSA Export Keys" can be exploited to trick web browsers into interacting with malicious websites. The problem affects a large number of web servers and clients and has thus received major media impact.

This discovery was made within the miTLS project, which is aimed at developing increasingly secure Internet authentication software. Pierre–Yves Strub, from the IMDEA Software Institute, and his colleagues have developed an automated technique to discover vulnerabilities in implementations of authentication protocols, and uncovered several vulnerabilities which, including the publicized FREAK attack, if unnoticed, could be exploited by hackers to compromise the security of Internet users and of the Internet as a whole.

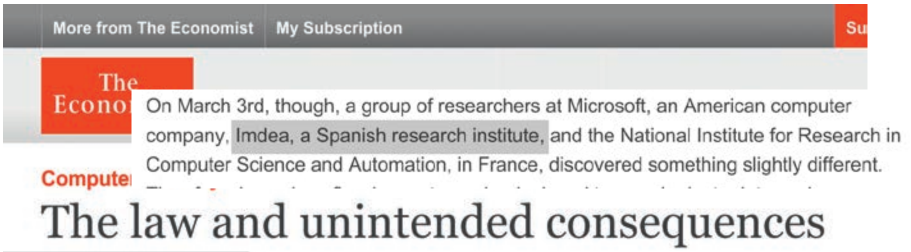
The researchers focused on the family of authentication protocols know as "Transport Layer Security" (TLS), which is the increasingly-popular successor to the ubiquitous "Secure Sockets Layer" (SSL) protocol family. By building formally-verified reference implementations of TLS protocols, they were able to systematically generate ill-formed responses which should be disallowed by the protocol, and test whether any of those responses were in fact accepted by existing implementations. Inadmissible responses suggest potential vulnerabilities, and were to converted into exploits in actual TLS implementations. "FREAK" is one of the vulnerabilities discovered.

This work was performed in collaboration with Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Alfredo Pironti, and Jean Karim Zinzindohoue of INRIA Rocquencourt, France, and Cedric Fournet and Markulf Kohleiss of Microsoft Research.

tack

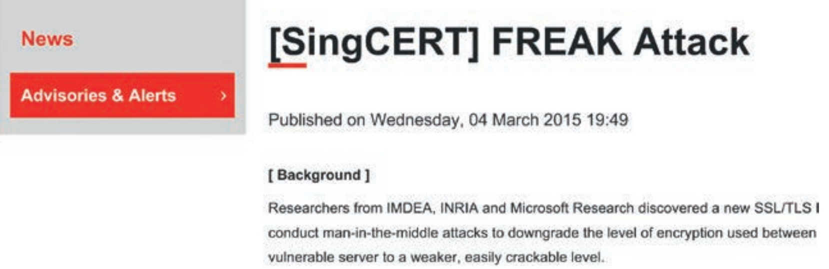
Related publications

[1] B. Beurdouche, K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, J.-K. Zinzindohoue “A Messy State of the Union: Taming the Composite State Machines of TLS.” in IEEE Symposium on Security and Privacy 2015, S&P 2015.



On March 3rd, though, a group of researchers at Microsoft, an American computer company, Imdea, a Spanish research institute, and the National Institute for Research in Computer Science and Automation, in France, discovered something slightly different.

The law and unintended consequences

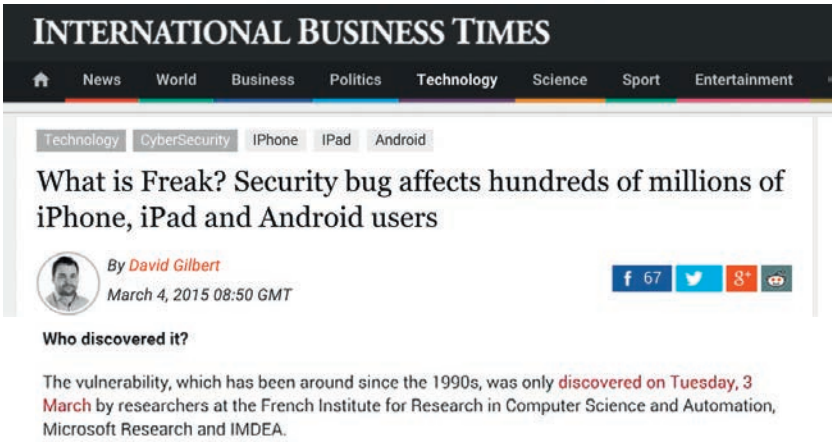


[SingCERT] FREAK Attack

Published on Wednesday, 04 March 2015 19:49

[Background]

Researchers from IMDEA, INRIA and Microsoft Research discovered a new SSL/TLS I conduct man-in-the-middle attacks to downgrade the level of encryption used between vulnerable server to a weaker, easily crackable level.



What is Freak? Security bug affects hundreds of millions of iPhone, iPad and Android users

By David Gilbert
March 4, 2015 08:50 GMT

Who discovered it?

The vulnerability, which has been around since the 1990s, was only discovered on Tuesday, 3 March by researchers at the French Institute for Research in Computer Science and Automation, Microsoft Research and IMDEA.

FREAK

“FREAK” flaw in Android and Apple devices cripples HTTPS crypto protection computer-aided

proofs

Computer-Aided Cryptographic Proofs

To deal with the rising complexity of cryptographic proofs, researchers from the IMDEA Software Institute and INRIA are developing tools for finding, writing, and checking cryptographic security proofs. One of the main results of this line of research is the EasyCrypt tool. EasyCrypt is dedicated to reasoning about relational properties of probabilistic computations with adversarial code and has been used to build machine-checked proofs of widely deployed cryptographic algorithms and protocols. It has also been used by multiple external research groups including MIT Lincoln Laboratory and the Microsoft Research-INRIA joint centre (in the context of the MiTLS project). Summer schools and workshops dedicated to this ecosystem took place at the University of Pennsylvania in July 2013, in Paris in November 2014 and at the University of Maryland in 2015 — attracting between 30 and 70 participants.

The team is exploring two main directions of research: applications to real-world cryptographic systems and automated analysis and synthesis of cryptographic constructions. In the first line of work, 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 [6]. Another recent achievement is a certifying compiler that enhances implementations of algorithms such as AES or Keccak with countermeasures against differential power analysis at arbitrary orders [2]. The second line of work has recently attracted funding from the US Office of Naval Research (ONR). The project, which is called *SynCrypt* and involves the IMDEA Software Institute, Stanford University, and University of Pennsylvania, started in 2015 and has already made significant progress. In collaboration with researchers at University of Pennsylvania, researchers at the IMDEA Software Institute have developed an automated toolchain [4] to synthesize and analyze structure preserving signatures in the generic group model. The toolchain has lead to the discovery of a new scheme with improved efficiency compared to existing constructions. Moreover, they have also applied synthesis techniques to discover new fault attacks on elliptic curve implementations [3]; 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 col-

cryptographic

laboration with researchers at INRIA, researchers at the IMDEA Software Institute have also developed an automated tool for proving the security of pairing-based cryptographic constructions in the standard model. The tool can be used by cryptographers without any previous knowledge of formal methods and is based on a logic that formalizes standard reasoning principles in pen-and-paper proofs.

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] Gilles Barthe and Sonia Belaïd and François Dupressoir and Pierre-Alain Fouque and Benjamin Grégoire and Pierre-Yves Strub, "Verified Proofs of Higher-Order Masking," in 34th European Conference on Advances in Cryptology, Eurocrypt 2015.

[3] 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.

[4] G. Barthe, E. Fagerholm, D. Fiore, A. Scedrov, B. Schmidt, M. Tibouchi, "Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds", in IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2015.

[5] G. Barthe, B. Grégoire, B. Schmidt, "Automated Proofs of Pairing-Based Cryptography", in 22nd ACM Conference on Computer and Communications Security, CCS 2015.

[6] 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.

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 EIT Digital (formerly known as 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.

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

During 2015, the emphasis was on detection on mobile devices that may be present on the enterprise network and may have been compromised. A showroom was also created in Milan to demonstrate the technology. After nearly two years of developement and testing, in December 2015 the CADENCE system was launched commercially. It is offered by Reply Communications Valley, with the support of the IMDEA Software Institute and TNO, as part of their security services to Italian clients in the banking and energy sectors.

detection

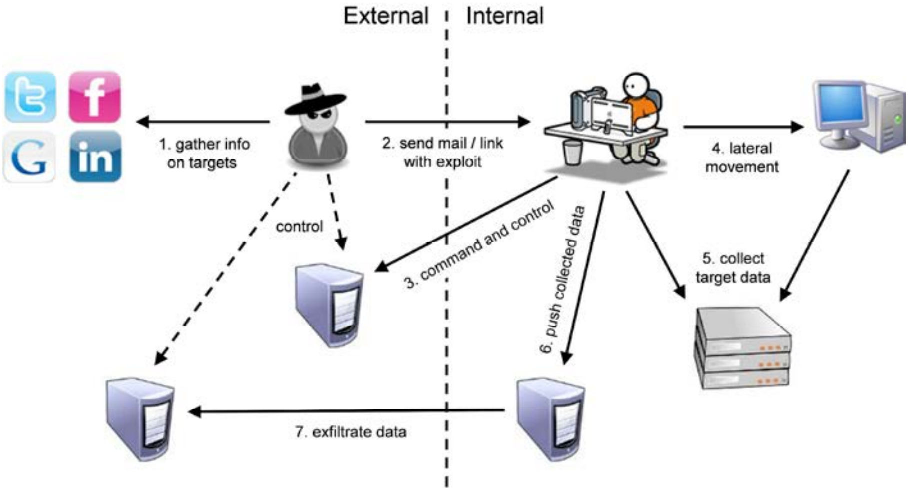
Related publications

[1] Antonio Nappa, M. Zubair Rafique, and Juan Caballero. "The MALICIA Dataset: Identification and Analysis of Drive-by Download Operations" In International Journal of Information Security, June 2014

[2] 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.

TNO innovation for life

Reply Living network



medals in verification competition

Medals in International Verification Competition

The International Competition on Software Verification (SV-COMP) is a driving force for the invention of new methods, technologies, and tools for the automated verification of computer software. Software verification is an unarguably important research area as society becomes more and more dependent on its correct functionality: software bugs can cost lives and great monetary loss. Though the goal of verified software has existed since the dawn of computer science, the technology enabling widespread use of software verifiers has been extremely challenging to develop, due to fundamental philosophical limitations, practical engineering obstacles, and the challenge in surmounting both simultaneously. SV-COMP aims to advance software verification technology by bringing together the top international minds.

This year marked the 4th annual installment of an increasingly-competitive event, in which 22 entries from top research institutions including New York University, Ecole Normale Supérieure (ENS) of Paris, University of Freiburg, Tsinghua University, Microsoft Research, and the IMDEA Software Institute competed across 13 categories of software verification problems.

Each competition entry is a computer program called a “verifier”, and each “problem” is a computer program whose correctness must be verified by the verifier. The verifiers are submitted as executable code, and the problems are provided as source code written in the C programming language. The verifiers classify problems either as “correct”, “incorrect”, or “unknown”, within a time limit of 900 seconds per problem. Points are awarded according to the accuracy of classification. In each problem category, the three highest-scoring verifiers are awarded medals: gold, silver, and bronze.

In collaboration with the University of Utah and Microsoft Research, the IMDEA Software Institute’s competition entry, named SMACK+Corral, was awarded medals in four categories — two gold, one silver, and one bronze — placing it among the top-performing verifiers. Only one entry earned more gold medals, and only three entries earned more medals total.

international

ETAPS
EUROPEAN JOINT CONFERENCES ON THEORY & PRACTICE OF SOFTWARE

SOFTWARE ANALYSIS RESEARCH LABORATORY

Microsoft Research

Technically, SMACK+Corral is the fusion of two programs. SMACK is an open-source project led by Zvonimir Rakamaric of the University of Utah, and Michael Emmi of the IMDEA Software Institute. The role of smack is to translate the C-language verification problems into mathematical representations which can be more-easily processed by automated logical-reasoning engines known as “theorem provers”. Corral, developed by Microsoft Research, applies novel reasoning algorithms to decide whether the given mathematical representation should be classified as “correct”. Combined, the two function as a powerful verifier of C-language programs.

The SV-COMP 2015 post-competition event was held on the week of April 13th, 2015, as part of the 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), in London. The event included a short presentation by the authors of each entry, and an official announcement of the competition results.

Related publications

[1] A. Haran, M. Carter, M. Emmi, A. Lal, S. Qadeer, and Z. Rakamaric. SMACK+Corral: A Modular Verifier. In Proc. 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS ’15). Springer, 2015.

[2] Z. Rakamaric and M. Emmi. SMACK: Decoupling Source Language Details from Verifier Implementations. In Proc. 26th International Conference on Computer Aided Verification (CAV ’14). Springer, 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. This allows raising energy consumption to a first-class issue for programmers and adding energy-related tools to the programmer's toolbox.

The results of the project include a number of techniques and tools that enable this energy transparency, such as, e.g., a multi-level static program analysis [3,7,9] that estimates the energy consumed by programs as functions on input data size. The analysis is performed at compile-time (using abstract interpretation), i.e., without actually running the programs [9], and uses low-level models of machine instructions or basic blocks [2] to infer 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 [8], and program optimization techniques [4,5,6] that exploit useful features offered by current hardware together with task scheduling techniques for multi-core systems. Most recently, a novel tool for profiling parametric accumulated cost statically has been developed. It is a more valuable aid for energy-aware software development than the traditional resource analyses, as it allows identifying the parts of a program that should be optimized first, because of their greater impact on the total energy consumption.

Although the energy savings achieved by applying the techniques and tools mentioned above can be arbitrarily large, depending on the extent to which a program is designed

sparency

taking energy efficiency into account and uses energy saving features, our experimental results with case studies show increased energy efficient by a factor of 6% to 50%. In addition, an estimate from Intel is that energy-efficient software can realize savings of a factor of three to five beyond what can be achieved through energy efficient hardware.

Current work focuses on 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 developing a set of recommendations for the integration of such energy-aware tools in the software life-cycle.

Related publications

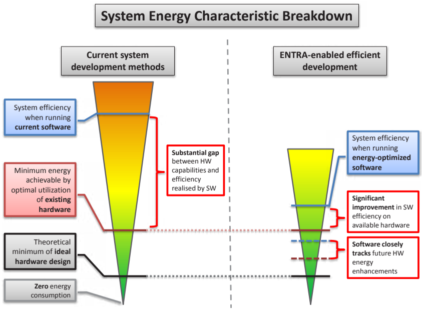
[1] R. Haemmerlé, P. Lopez-Garcia, U. Liqat, M. Klemen, J. P. Gallagher and Manuel Hermenegildo. *A Transformational Approach to Parametric Accumulated-cost Static Profiling*. 13th International Symposium on Functional and Logic Programming (FLOPS 2016), volume 9613 of LNCS, pages 163-180. Springer, March 2016.

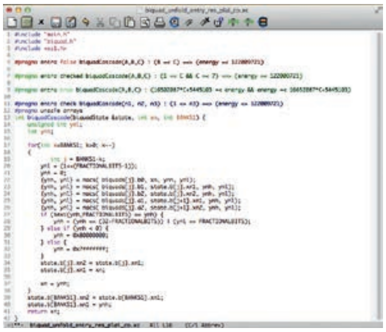
[2] U. Liqat, K. Georgiou, S. Kerrison, P. Lopez-Garcia, M. V. Hermenegildo, J. P. Gallagher, and K. Eder. Inferring Energy Consumption at Different Software Levels: ISA vs. LLVM IR. Foundational and Practical Aspects of Resource Analysis. Fourth International Workshop FOPARA 2015, Revised Selected Papers, Lecture Notes in Computer Science, Springer. To appear.

[3] Z. Banković and P. Lopez-Garcia. *Stochastic vs. Deterministic Evolutionary Algorithm-based Allocation and Scheduling for XMOS Chips*. Neurocomputing, Vol. 150, pages 82–89, Elsevier, February 2015.

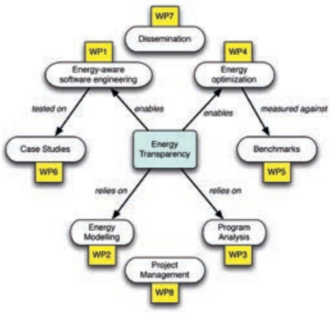
[4] U. Liqat, S. Kerrison, A. Serrano, K. Georgiou, P. Lopez-Garcia, N. Grech, M. V. Hermenegildo, and K. Eder. Energy Consumption Analysis of Programs based on XMOS ISA-level Models. Logic-Based Program Synthesis and Transformation, 23rd International Symposium, LOPSTR 2013, Revised Selected Papers, Lecture Notes in Computer Science, Vol. 8901, pages 72–90, Springer, 2014.

[5] 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.


System Energy Characteristic Breakdown
Current system development methods
ENTRA-enabled efficient development
System efficiency when running current software
Minimum energy achievable by optimal utilization of existing hardware
Theoretical minimum of ideal hardware design
Zero energy consumption
Substantial gap between HW capabilities and efficiency realised by SW
System efficiency when running energy-optimized software
Significant improvement in SW efficiency on available hardware
Software closely tracks future HW energy enhancements



```
#include "main.h"
#include "biquad.h"
#include <xs1.h>

#pragma entry false biquadCascade(A,B,C) : (B == C) ==> (energy == 122000721)

#pragma entry checked biquadCascade(A,B,C) : (1 =< C && C =< 7) ==> (energy == 122000721)

#pragma entry true biquadCascade(A,B,C) : ([illegible]*C+5445183 =< energy && energy =< [illegible]*C+5445183)

#pragma entry check biquadCascade(A1, A2, A3) : (1 == A3) ==> (energy == 122000721)
#pragma unsafe arrays
int biquadCascade(biquadState &state, int xn, int BANKS1) {
    unsigned int ynl;
    int ynh;

    for(int i=BANKS1; i>=0; i--)
    {
        int j = BANKS1-i;
        ynl = (1<<(FRACTIONALBITS-1));
        ynh = 0;
        {ynh, ynl} = macs( biquads[j].b0, xn, ynh, ynl);
        {ynh, ynl} = macs( biquads[j].b1, state.b[j].xn1, ynh, ynl);
        {ynh, ynl} = macs( biquads[j].b2, state.b[j].xn2, ynh, ynl);
        {ynh, ynl} = macs( biquads[j].a1, state.b[j+1].xn1, ynh, ynl);
        {ynh, ynl} = macs( biquads[j].a2, state.b[j+1].xn2, ynh, ynl);
        if (sext(ynh,FRACTIONALBITS) == ynh) {
            ynh = (ynh << (32-FRACTIONALBITS)) | (ynl >> FRACTIONALBITS);
        } else if (ynh < 0) {
            ynh = 0x80000000;
        } else {
            ynh = 0x7fffffff;
        }
        state.b[j].xn2 = state.b[j].xn1;
        state.b[j].xn1 = xn;

        xn = ynh;
    }
    state.b[BANKS1].xn2 = state.b[BANKS1].xn1;
    state.b[BANKS1].xn1 = ynh;
    return xn;
}
```



editor
imdea software institute

graphic design
base 12 diseño y comunicación

photos on pages 13 and 14
Daniel Schäfer

photo in page 11
Víctor Castelo

legal deposit number
M-8312-2016

Comunidad de Madrid

EUROPEAN UNION
STRUCTURAL FUNDS

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

www.software.imdea.org

annual report