imdea **software** institute

science and technology
for developing better software

institute
iMdea
software

annual report

2017

www.**software**.imdea.org

foreword

Manuel Carro
Director, IMDEA Software Institute
April 20, 2018

annual report 2017

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 currently as relevant as ever, and software-related technology indeed has an immense potential for raising industrial competitiveness, opening whole new business areas, creating high added-value jobs, protecting our security and privacy, 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.

The key asset of the Institute is its people: its researchers and support staff. While this is true for any scientific discipline, it is more so in an area where, except in certain subareas, the cost of experimentation facilities is not as high as in other sciences. In line with the observation that people are key, the Institute has continued to attract to Madrid top talent worldwide, and during 2017 it included 16 faculty (one half-time), 2 associate faculty, 10 postdocs, 1 senior visitor, 22 research assistants, 19 interns, 10 project staff, and 9 staff members, from 18 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, 209 international researchers have visited and given talks at the Institute to date.

During 2017 Institute researchers have published 62 refereed publications in some of the top venues in the field, such as POPL, PLDI, ACM CCS, CRYPTO, EUROCRYPT, IEEE S&P, USENIX Security, PODC, CAV, ICFP, LICS, given 23 invited talks in international conferences, 32 invited seminars and lectures, chaired 10 program committees, and participated as members in 39 program committees and 24 boards of journals and conferences, in addition to being conference or program chairs of 14 conferences. The Institute has received 17 best paper awards or mentions in the last 5 years.

The Institute has also participated during 2017 in 29 funded research projects and contracts, and its researchers were awarded 14 fellowships. Thirteen of these projects come from international agencies and companies, five have direct industrial funding, and eleven of them involve collaboration with companies of all sizes, both Spanish and international. These companies include, among others, ATOS, Google, IBM, INDRA, Microsoft, RedBorder, Relational, Reply Communications Valley, Scytl, and Zemsania. The Institute has also started to work in 2017 in the commercialization of the results of the EIT Digital AntiFraud project with the Italian company Reply Communication Valley.

This year, the Institute further strengthened its strategic partnership with EIT Digital, the European Institute of Innovation and Technology's KIC on Information Technologies, and especially with the members of the Madrid Node: Atos, Ferrovial, Indra, Nokia-Spain, Telefónica, and UPM. In 2017, the Madrid Node of EIT Digital was promoted to full node status (it was previously an *Associated Partner Group*). The official opening of the Madrid node in March had the participation of the Spanish Minister for Education Mr. Íñigo Mendez de Vigo, the EU Commissioner for Education, Youth, and Sport, Mr. Tibor Navracsics, EIT Digital's CEO Mr. Willem Jonker, as well as other representatives of the Spanish and Regional Governments, and Universities and companies in the Madrid region. The promotion to full node made it possible the expansion of the node and a significant increase of its activities. Many of these activities take place at the Co-Location Center hosted at and run by the IMDEA Software Institute, and include innovation and entrepreneurship training, business development activities, coaching for startups and scale-ups, and startup hosting.

In 2017, the Institute continued its strong collaboration with Telefónica through our Joint Research Unit, whose activity has been framed during 2017 within the realm of EIT Digital innovation activities.

I would like to thank 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. Last, but by no means least, I would like to thank very specially Manuel Hermenegildo, who was Director of the Institute since its very start until May 2017. Without his leadership, clarity of vision, and never-ending energy, the Institute could not have reached in such a short time the level of international recognition it has now. We all are in debt to him.

t a b l e o f
c o n t e n t s

table of contents

annual report
2017

general presentation

annual report 2017

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 the methods, languages, and tools that will allow the cost-effective development of software products with sophisticated functionality and high quality, i.e., software which is 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: according to European Commission data the overall software and software-based services

(SSBS) market in the EU28 region was worth €229 billion in 2009 and by 2020 it will amount to nearly €290 billion. The average yearly growth of the SSBS industry in Europe is expected to be 2.9% between 2015 and 2020. Software sector employment in the EU grew by 16.1% between 2008 and 2013, as opposed to a decline in employment in the total business economy of about 3.4% and high productivity (measured in value added per employee) characterizes the SSBS companies. This vividly illustrates the huge potential of the European SSBS industry to drive economic growth and create jobs. The same source states 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.

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, 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 cyberattacks in the European Union is in the order of billions each year. In 2013 a single data breach cost a U.S. 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 cyberattacks 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

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.

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, verification, validation, evolution and 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, coopera-

tion 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. It normally meets twice a year. In the interim, Board-level decisions are delegated to the **Standing Committee** of the Board. The **Director**, who is the CEO of the Institute, is appointed by the board 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.

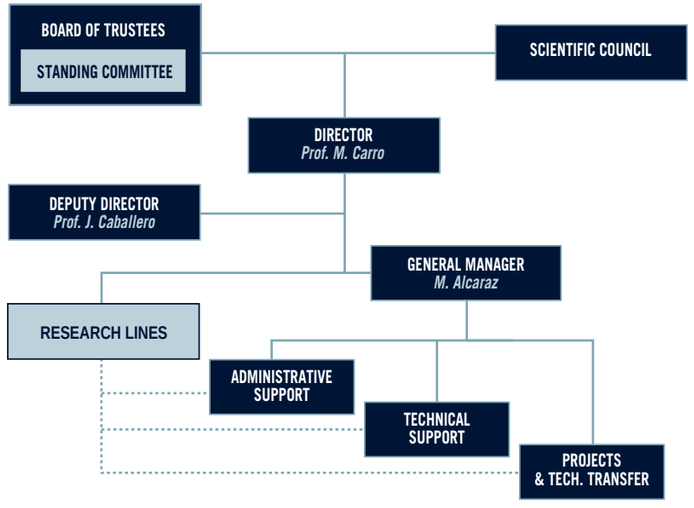


Figure 1.1. Governance and management structure of the IMDEA Software Institute.

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

The name of the Regional Ministry that the Institute depends on has been changed to *Regional Ministry of Education and Research*. The Councilor, Mr. Rafael van Grieken, continues in the Board of Trustees in his position. The Regional Ministry has also undergone an internal reorganization by splitting the Directorate general for Universities and Research. A new post of Director General for Universities and Higher Art Studies has been created and the corresponding official, Mr. José Manuel Torralba Castelló, selected by the Regional Government as member of the Board of Trustees. A new post for Director General for Research and Innovation was created, and its appointee, Mr. Alejandro Arranz Calvo, selected as member of 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 and Research, Madrid Regional Government, Spain.

MADRID REGIONAL GOVERNMENT

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

Ilmo. Sr. D. Alejandro Arranz Calvo
Director-General for Research and Innovation, Madrid Regional Government, Spain.

Ilmo. Sr. D. José Manuel Torralba Castelló
Director-General for Universities and Higher Art Studies, 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. Francisco Javier Soriano Camino
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. Luís Moniz Pereira
Universidade Nova de Lisboa, Portugal.

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

Prof. Roberto Di Cosmo
Université Paris Diderot and INRIA, France.

EXPERT TRUSTEES

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

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

INVITED MEMBERS FROM INDUSTRY

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

Telefónica I+D
Mr. Luis Ignacio Vicente del Olmo, Return on Innovation Manager and Head of Telefónica Patent Office, and Estanislao Fernández González-Colaço.

Elecnor Deimos
Mr. Ismael López and *Mr. Miguel Lizondo.*

Atos
Ms. Clara Pezuela, Head of IT Market.

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 headquarters building, which was officially inaugurated in July 2013, in the Montegancedo Science and Technology Park. These premises offer an ideal environment for fulfilling the mission of attraction of talent, research, and technology transfer. They include 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. The building also provides ample space for strategic activities such as the Madrid Co-location Center of the EIT Digital KIC, the IMDEA Software-Telefónica Joint Research Unit, and other joint research units with industry, such as the former IMDEA Software-Microsoft Joint Research Center. 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 School of Computer Science 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 Institute's location also provides convenient access to the other Madrid universities and IMDEAs.

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

annual report
2017

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 high-impact area of ICT, IMDEA Software is committed to 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 in areas of common interests across specific research projects. In particular, the Institute has established close ties with Telefónica, Indra, and Atos, which have led to a number of strategic cooperation initiatives. An important instance of these initiatives was the joint establishment of the Spanish Associate Partner Group of EIT Digital, with the added participation of UPM, the Fundación General UPM, Nokia Spain, and Ferrovial, that evolved towards the status of Full Node (started in January 2017) under the leadership of 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 Ph.D. level), innovation, and entrepreneurship. In addition, the Institute has established with Telefónica the *Telefónica-IMDEA Software Joint Research Unit* 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 and MadridNetwork in the Madrid Region, the Internet of the Future *Es.Internet* Spanish platform, the Spanish Technology Platform for Security and Trust (eSEC, as part of the AMETIC Association), the Spanish Network of Excellence on Research on Cyber Security (RENIC), and the European Cyber Security Organization (ECSO) that implements the Cyber Security Public-Private Partnership (cPPP) of the European Commission. 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, together with the licensing of such technology (e.g., the CADENCE technologies have been licensed to Communication Valley Reply), 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 started time ago); GGA; EasyCrypt, ZooCrypt, and Masking (the last 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 presented their research results to BBVA, Telefónica I+D, Ericsson, GMV, INDRA, IBM, Canal de Isabel II, Interligare, or Lingway, among many others), access to the Institute's researchers as consultants, participation of company staff in Institute activities, etc.

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
Ph.D. 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
NEXTLEAP	H2020	Merlinux
ELASTEST	H2020	Fraunhofer, Telecom Italia, Atos, Tikal Technologies, IBM Ireland, Relational
DataMantium	MINECO	Scytl
AxE Javascript	MINECO	Scytl
HC@WORKS	EIT	Atos, Thales, Engineering, CEA List
SMAPPER	EIT	Telecom Italia, Backes SRT
ANTIFRAUD	EIT	Reply SpA
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
Contracts	NEC	NEC Laboratories Europe GmbH
Contracts	INDRA	INDRA Sistemas S.A.
Contracts (Cyber 4.0)	RedBorder	RedBorder
Contracts (RiskIoT)	Nextel	Nextel S.A. Ingeniería y Consultoría

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).
- NEC Laboratories Europe GmbH (activities starting on 2018).

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) included hosting 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 existing Masters ("MUSS") and Ph.D. programs ("DSSC") at UPM. In them, researchers from the Institute can teach through a "Venia Docendi", i.e., a permission to teach, and be Ph.D. thesis advisors. Most research assistants at the IMDEA Software Institute obtain their Masters and Ph.D. following these programs. Under the agreement with the Consejo Superior de Investigaciones Científicas, two researchers—César Sánchez and Pedro López—have a dual appointment 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 has included 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 (now finished) 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. Manuel Hermenegildo, Director of the Institute until the second half of 2017, was Vice-President of Informatics Europe. In addition, the Institute was a member of ERCIM, the *European Research Consortium for Informatics and Mathematics* and SpaRCIM, the *Spanish Research Consortium for Informatics and Mathematics*.

2.3. EIT Digital

EIT Digital is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT). EIT Digital includes some of the leading educational, research, and industrial actors in the ICT innovation ecosystem in Europe, and its mission is to combine educational, research, and industrial tools and activities to drive and foster ICT innovation on the European scale in the following strategic areas: Digital Industry, Digital Cities, Digital Wellbeing, Digital Infrastructure and, starting in 2018, Digital Financing. These areas are complemented by integrated and innovation-driven Master and Doctoral Schools, EIT Digital acceleration programs, and a Professional School.

In June 2013, IMDEA Software officially became an Associate Partner of EIT Digital (formerly known as EIT ICT Labs), becoming the first Spanish organization to enter its Pan-European network of the then 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).

One of the key goals of IMDEA Software as the Spanish Associate Member was 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 included some of the most prominent players in the ICT innovation arena, such as Atos, Indra, Telefónica, and the Technical University of Madrid (UPM), towards a fully operational EIT Digital node. This goal was achieved in September 2016, with the positive vote for the candidature at the EIT Digital General Assembly and the start of operations as a full node started on January 1, 2017, when, after a process started during the previous year, Madrid was recognized as full node within EIT Digital.

This change of status allowed the Madrid Node to have the same rights as the eight other European Nodes of EIT Digital, which offers great opportunities for Spain in driving forward digital transformation across Europe and made it possible to significantly increase the presence and leadership of the Spanish partners in all activities and initiatives of EIT Digital, thus extending the impact of Spain on innovation at the European level and strengthening the development of digital innovation in Spain. This step marked the completion of a mission that spanned over the years 2013 to 2016, in which nearly €20 million were invested in Spain. Becoming a full Node enabled a faster expansion of activities, as is demonstrated by the fact that €15 million is being invested in 2017 alone in Spanish Innovation & Entrepreneurship, as well as Entrepreuneurial Education activities.

The opening ceremony for the new node was held on March 2, 2017, with the attendance of, among others, Mr. Tibor Navracsics, Commissioner for Education, Culture, Youth and Sport, Mr. Íñigo Méndez de Vigo, Spanish Minister for Education, Culture, and Sport, and Mr. Willem Jonker, CEO of EIT Digital. The opening, which included a showcase of technology closely tied or developed inside EIT Digital, showed the closer integration of the Spanish innovation ecosystem into the European market through the new EIT Digital Node.

In addition to the initial ecosystem, two new partners, Ferrovial and Nokia Spain, joined the node in 2017, and three others (Agromán, Innovalia, Centro de Innovación de Infraestructuras Inteligentes — CI3) were accepted by the Node Strategy Board and the EIT Digital Steering Board to become partners of EIT Digital starting Jan. 1, 2018.

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 the interaction with regional and national governments, and boosting and creating synergies between the entrepreneurship initiatives and mechanisms led by the members of the Spanish node and beyond.

IMDEA Software has participated in the EIT Digital Business Plan for 2017 with the following activities:

- Research and innovation activity in the field of Digital Infrastructure, Cybersecurity (project Online Banking Anti-Fraud Monitoring – 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 node, and has the objective of fostering innovation, technology

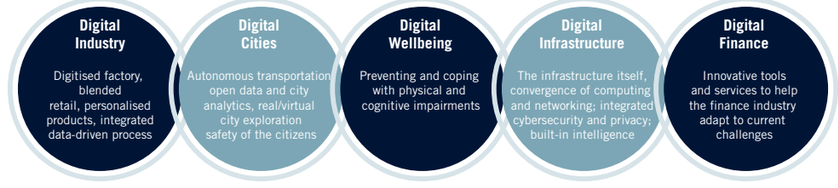
transfer, and entrepreneurship in Spain. The CLC is equipped with ample office space and meeting facilities, workspaces for start-ups, and work and collaboration areas for the students in the EIT Digital masters and doctoral programs. In addition to the organization and participation in relevant events devoted to innovation (e.g., matchmaking events on cybersecurity with large corporations), the CLC also hosts startups and scale-ups. During 2017 three companies, participating in the EIT Digital Accelerator Program, have been coached and hosted at the CLC: Coowry, Redborder, OpenCloud Factory and eIdentity.

- Consolidation of the Madrid Business Developers (BD) segment which is part of the EIT Digital BDA 50-strong specialist 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. During 2017 the team scouted more than 250 companies in Spain and Portugal.

- Run the EIT Digital Doctoral Training Center and gave support to increase the Master Program with two more programs, in cooperation with UPM. The masters program 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 leading business partners in European top research facilities. The CLC hosts EIT Digital lectures on Innovation and Entrepreneurship and offers students a space to meet and work, surrounded by the vibrant EIT Digital ecosystem.

- Organization of the pan-european ETI Digital Master School Graduation Ceremony. IMDEA Software was responsible for organizing the global graduation ceremony for more than 200 students and 700 invitees in 2017. The ceremony took place at the School of Civil Engineering of the Technical University of Madrid, with keynote speakers such as the President of the Technical University, Prof. Guillermo Cisneros, the CEO of Telefónica Research and Development, Mr. David del Val, and Director General of Minsait, Mr. Silviano Andreu. The gala dinner event took place in the *Casino de Madrid*, with speeches from the CEO of EIT Digital, Willem Jonker.

Action lines

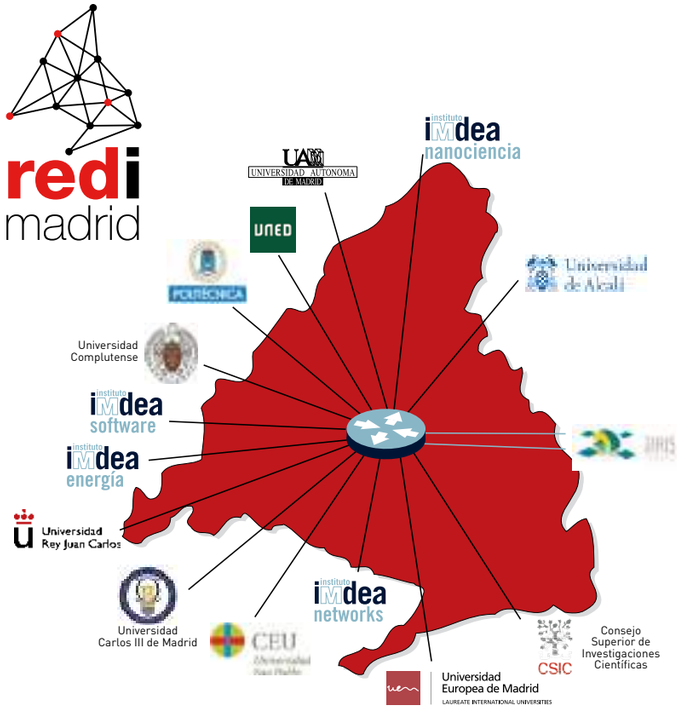


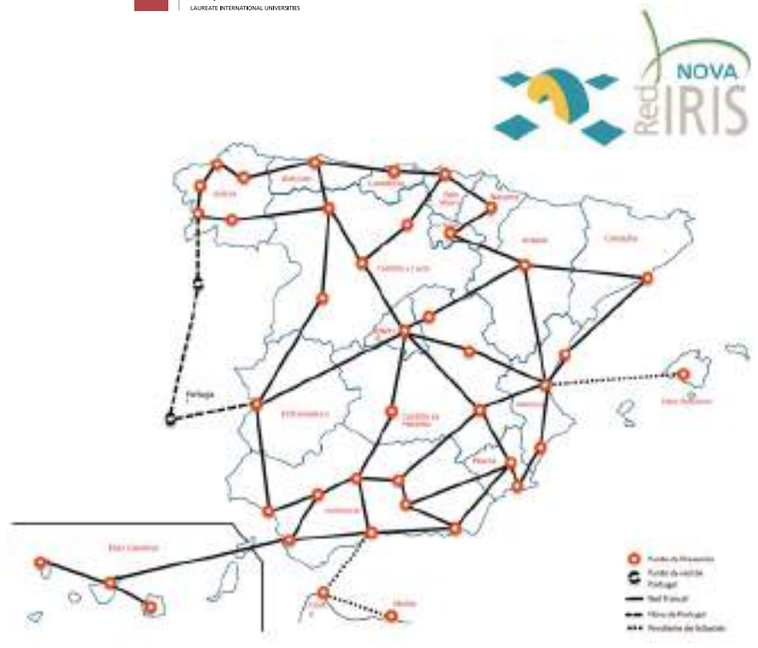
2.6. REDIMadrid

REDIMadrid is the data network for research and higher education that provides high-speed connectivity to universities and research centers within the Madrid region. REDIMadrid is funded by the Madrid Regional Government and managed by the IMDEA Software Institute. REDIMadrid provides the connected institutions, which include all public universities in the area of Madrid and the IMDEA research Institutes, with a highly-reliable, high-speed connection. The communication infrastructure provided by REDIMadrid allows these institutions to interact among themselves and to access the national network (RedIRIS), the European research network Géant, and the rest of the Internet. Public universities in the area of Madrid are provided several diversified connections at 10Gb per second using a physical deployment of metropolitan fiber-optic rings, which provides a highly reliable infrastructure that is easy to upgrade as technology does.

The *EIT Digital communication node*, hosted and operated by the IMDEA Software Institute, connects to the main points of presence of REDIMadrid using dark fiber acquired by RedIRIS as part of the RedIRIS-NOVA initiative, and operated by REDIMadrid with a pioneering prototype connection of 100Gbps.

In 2017, REDIMadrid continued with the expansion to a modern dark fiber network with the acquisition of a sequence of links that connect both points of presence of REDIMadrid (at CIEMAT and CSIC) with the main campuses of Universidad Carlos III and Universidad Rey Juan Carlos, and with the IMDEA Networks Institute. This acquisition allows providing redundant high-speed connectivity of the universities and centers in the south of the region to the backbone of REDIMadrid, and will facilitate future expansions to easily accommodate the connectivity needs of these centers for years to come. The deployment of this network started in 2017, and it is planned to finish during the first half of 2018, to continue with the acquisition of the corresponding optical and IP equipment.





research

annual report 2017

The research activities carried out by the IMDEA Software Institute address directly its core mission: to advance the technology and the scientific foundations that enable the cost-efficient development of software for tomorrow's computing platforms. That is, software with sophisticated functionality and high quality in terms of reliability, security, 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 and automotive software, to tools that explore energy consumption profiles at design time, which is fundamental for cost-effective software development in the mobile and embedded domains.

- 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 results include powerful multi-paradigm programming environments as well as novel language-based techniques for building provably secure concurrent and distributed systems.

- Our research on *Security and Privacy* delivers technology that enables computation, communication, and storage in open, untrusted, and malicious environments, such as the Internet of Things. Our results include novel cryptographic protocols and privacy-enhancing technology, as well as cutting-edge techniques for detecting and analyzing vulnerabilities and malicious activities 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). In particular, it is worth mentioning our novel *static profiling* techniques, which are more useful for resource-aware software development than standard resource usage analysis.

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 adaptable to different languages, hardware, and resources because it is built around a customizable static analyzer with a versatile assertion language, in combination with

dynamic techniques for modelling. 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" has been performed within the European project ENTRA.

3.2 Reliability of Concurrent and Distributed Software

In the past decade computing has undergone a radical shift: with the advent of multicore processors and cloud computing, concurrent and distributed programming have gone mainstream. Unfortunately, programmers find it particularly hard to write correct software using these paradigms, because reasoning about the behaviour of concurrent and distributed software is inherently difficult. Reasoning about concurrency requires a programmer to keep track of multiple threads of computation and interactions between them; distribution additionally requires considering computations located in different places and inevitable failures. This complexity makes it easy for programmers to make mistakes. It also makes traditional testing less effective in finding bugs, leading to unreliable software.

All this makes formal verification a more appealing technique for ensuring software reliability. However, new verification methods are needed to deal with modern concurrent and distributed software. 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 programs. 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 distributed software. These techniques are aimed at a wide range of aspects of modern software: asynchronous programs, lock-free algorithms, and cloud databases. Apart from building the foundations for reasoning rigorously about these aspects of modern concurrent and distributed 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 lock-free algorithms.

3.3 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 design 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. IMDEA Software researchers also develop techniques for reducing the overhead of run-time testing, both through combination with static analysis and through better implementation techniques.

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.

3.4 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 electronically available information endanger values we have traditionally cherished. The inference power of modern machine learning does not only directly threaten the most basic privacy expectations of citizens, governments and corporations, but can also impact people's freedom, ultimately creating an unbalance in power relations which in turn may damage our democratic society.

Therefore, a deep understanding of the implications for privacy of the explosion of, for instance, Big Data analytics, pervasive sensors (e.g., wearables or smartphones), per-

sonalized services (e.g., personalized medicine), or de-centralization approaches (e.g., blockchain based systems) 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 IT 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 IT 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 the best choices of system architecture and state-of-the-art privacy-preserving technologies when building IT 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 IT 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 control the amount of information leaked in shared genomic information, and a means to prove to a third party correctness of a computation over a set of data without this party learning any information about these data.

3.5 Fighting Cybercrime and Targeted Attacks

Cyberattacks are a huge challenge to developed societies and the Internet at large. Two main threats dominate this environment: *cybercrime* and *targeted attacks*. Cybercriminals focus on economies of scale by monetizing large numbers of compromised Internet-connected hosts and their users. Users of compromised hosts can be blackmailed to pay fees for recovering their data, previously encrypted by the attacker, or incited to buy licenses for rogue software of little value. Compromised hosts can be monetized as assets for, among others, sending spam, launching denial-of-service attacks, mining virtual currencies, faking user clicks on online advertisements, or as stepping stones to hide the attacker's real location.

Targeted attacks focus on high-value targets. They have become a focus of the security industry, which has coined a new term for them: *Advanced Persistent Threats* (APTs), which refers to highly determined, well-funded, cyber-attackers, who persistently target an individual, group, or 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 compromised Internet-connected computers. 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 and to collect data exfiltrated from the compromised hosts.

Researchers at the IMDEA Software Institute are developing novel defenses against cybercrime and targeted attacks. On the malware side, during 2016 we have performed,

in collaboration with Symantec Research, the first measurement of the distribution of potentially unwanted programs (PUP) such as adware and rogueware. Our analysis of 3.9 million Windows hosts showed that 54% are affected by PUP and that pay-per-install (PPI) services play a key role in their distribution. We have also developed AVClass, a massive malware labeling tool, which we have open-sourced to help researchers improve their threat intelligence analysis. On the server side, during 2016 we have developed novel active probing techniques to detect silent Web reverse proxies, which can be used by attackers to hide the location of their Web servers.

3.6 Cryptography for Next Generation Cloud Computing

Cloud computing is a fast-growing paradigm in which users lease computation resources from powerful service providers. Virtual machines, remote storage, email, web-content, databases are only some examples of services that are nowadays outsourced to the Cloud. This paradigm is very appealing to individuals and businesses due to its significant benefits: reduced IT costs, increased mobile productivity, convenient access to remote resources from multiple devices, different geographic locations, etc. The downside of cloud computing is that keeping a clear control over the data and the computations that are outsourced to the Cloud is becoming more difficult. This new working scenario exposes users to faults and attacks that are out of 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 user 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 user 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 techniques 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 put their privacy and integrity at risk.

3.7 Computer-Aided Cryptographic Proofs

The goal of modern cryptography is to design efficient algorithms that achieve some desired functionality, and to formally prove that these algorithms guarantee a set of security requirements. Over the years, the realm of cryptography has expanded from basic primitives such as encryption, digital signatures or key exchange, to more elaborate functionalities, such as zero-knowledge protocols, or secure multi-party computation, to name a few. In many cases, these elaborate functionalities can only be built through the combination of several, elementary, cryptographic primitives. As a consequence, also proving the security of these more complex functionalities have become significantly more involved and more difficult to check. Furthermore, because cryptographic proofs are very complex, it is common practice to argue the security of cryptographic protocols at an algorithmic level, rather than at the level of implementations. This has the consequence that implementations of well-known and provably-secure cryptographic protocols are vulnerable to attacks, and regularly fail to provide their intended security guarantees.

Researchers at IMDEA Software are actively working to solve these issues, by advancing computer-aided cryptography. The main goal of this research is to develop foundations and tools that allow building and verifying the security of cryptographic protocols in an automated fashion. Additionally, it aims to verify the security guarantees at the level of implementations, thus reducing the gap between the traditional, theoretical, provable security approach and the cryptographic engineering practices.

In this domain, IMDEA researchers have explored techniques based on programming languages that allow protecting implementations of cryptographic algorithms against important classes of side-channel attacks, such as cache attacks, differential power analysis attacks and timing attacks. Notably, they developed a methodology for proving

security of implementations against timing attacks, and have shown an application of their methodology to a key component of a proof-of-concept implementation of TLS, one of the most widely used cryptographic protocols on the Internet. Their research in this area also allowed them to unveil and report an implementation bug in the S2N library by Amazon Web Services Labs.

In a related research line, IMDEA researchers have demonstrated how the methods and tools of computer-aided cryptography can be used to reason about differential privacy, a promising formal approach to data privacy, which provides a quantitative bound on the privacy cost of an algorithm that operates on sensitive information.

3.8 Side-Channel Attacks and Countermeasures

Side channel attacks break the security of programs by exploiting signals that are unwittingly emitted during their execution. Examples of such signals are the consumption of power, memory, and execution time. Among those signals, execution time stands out because it can be measured and exploited remotely and thus poses a threat against open, distributed systems such as the Internet.

Three landmark attacks illustrate the evolution of timing attacks from an academic stunt to a fundamental and hard-to-mitigate attack vectors: (1) a remote attack against secret-dependent branches that recovers full RSA keys from timing measurements of the TLS handshake; (2) an attack (coined FLUSH+RELOAD) against last-level caches that recovers most of the key bits from timing measurements of memory accesses during of a single RSA encryption; and (3) a class of attacks (coined SPECTRE and MELTDOWN) against the combination of speculative execution and caching that enables unprivileged processes to bypass Kernel memory isolation and that affects most modern CPUs.

Different countermeasures have been proposed to close the different kinds of channels. They include ensuring that control flow, memory access-patterns, and execution time of individual instructions are independent of confidential data, or to carefully restricting the sharing of resources, such as caches or translation look-aside buffers.

There are two key challenges involved with this approach. First, writing constant-time software is hard because it needs the use of low-level programming languages and forces developers to deviate from conventional programming practices. Second, constant-time software typically comes with significant slowdowns and is not a general-purpose solution in performance-oriented markets.

In our research at the IMDEA Software Institute we address both challenges: first, we develop tools that help with the compilation and verification of constant-time software. Second, we are developing techniques for rigorously quantifying leaks. This is needed for exploring middle grounds between constant-time software and aggressively tuned code, and is a fundamental building block for designing and evaluating more efficient defenses.

people

annual report 2017

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.

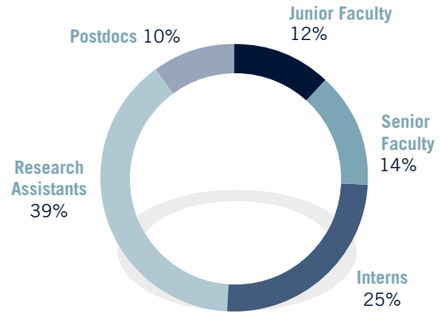


Figure 4.1. Type of position, all researchers.

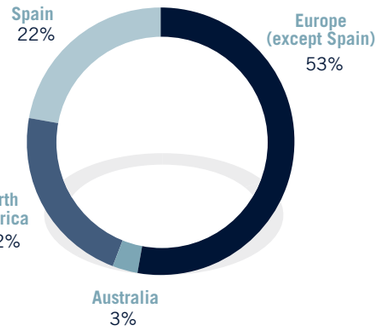


Figure 4.2. Where PhD was obtained (by continent + Spain).

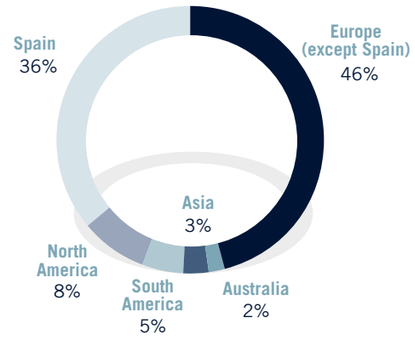


Figure 4.3. Location of previous institution, all (by continent + Spain).

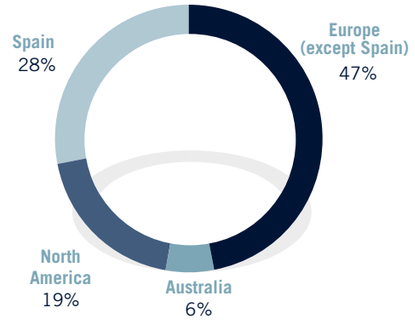


Figure 4.4. Location of previous institution of researchers at or above postdoc level (by continent + Spain).

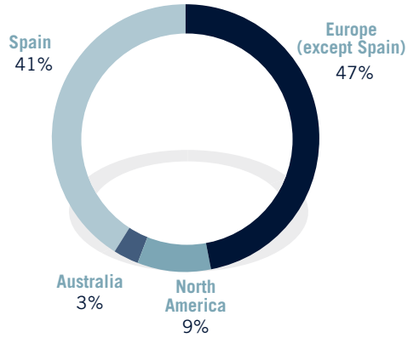


Figure 4.5. Nationality of researchers at or above postdoc level (by continent + Spain).

Status

In 2017, the scientific staff of the Institute was composed of 11 senior faculty (full or associate professors, one part-time), 5 junior faculty (tenure-track or researchers), 10 postdoctoral researchers, 2 research programmers, 22 research assistants (Ph.D. candidates), 13 project staff, 3 system support staff, and 3 administrative support members. A total of 2 senior faculty visitors and 18 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 2017 (where 24% were faculty members vs. 76% non-faculty). Figure 4.2 summarizes where these researchers obtained their Ph.D. (by continents plus Spain), and Figure 4.3 shows the location where the Institute researchers were working previously to joining IMDEA. Finally, Figure 4.5 presents the nationalities of researchers at or above the postdoc level.

faculty

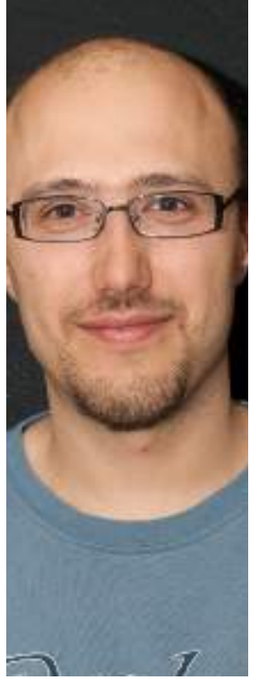
Manuel Carro

Associate Research Professor and Scientific Director

Manuel Carro received his Bachelor degree in Computer Science from the Technical University of Madrid (UPM), and his Ph.D. degree from the same University in 2003. He is currently an Associate Professor at the Technical University of Madrid, Associate Research Professor at the IMDEA Software Institute and, since May 2017, its Director. He also acts act deputy representative of IMDEA Software at Informatics Europe and representative of the Institute at the Node Strategy Committee of EIT Digital Spain. He has previously been Deputy Director at the IMDEA Software Institute, representative of UPM at the NESSI and INES technological platforms, representative of UPM at SpaRCIM, deputy representative of IMDEA Software at ERCIM, and CLC Manager and Scientific Coordinator of the Madrid Node of EIT Digital. He has published over 80 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, including conference chair of ICLP 2014 and PC chair of ICLP 2016, the flagship conference in the field of Logic Programming. He has 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 several national and a regional research projects. He has completed the supervision of four Ph.D. theses 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 to express non-monotonic knowledge and reasoning and to improve the quality of software production, the analysis of service-based systems, and the effective usage of formal specifications in teaching programming. He has long been interested in parallel programming, parallel implementations of declarative languages, and visualization of program execution.



Juan Caballero

Associate Research Professor and Deputy Director

Juan Caballero received his Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University, USA, in 2010. He joined the Institute in November 2010 as an Assistant Research Professor and was promoted to Associate Research Professor in December 2016. He was appointed Deputy Director of the Institute in September 2017. Prior to joining the Institute, Juan was a visiting graduate student researcher at University of California, Berkeley for two years. Juan also holds an M.Sc. in Electrical Engineering from the Royal Institute of Technology (KTH), Sweden, and a Telecommunications Engineer degree from Technical University of Madrid (UPM), Spain. His research regularly appears at the top venues in computer security and has won two best paper awards at the USENIX Security Symposium and the DIMVA Most Influential Paper 2009-2013 award. He is a recipient of the La Caixa fellowship for graduate studies. He has been principal investigator of multiple national and European projects. He is an Associate Editor for the ACM Transactions on Privacy and Security (TOPS) journal and a member of the steering committee for the DIMVA, ESSOS, and JNIC conferences. He has been program chair or co-chair for ACSAC, DIMVA, DFRWS, ESSOS, and EuroSec. He has been a member of the technical committee for the top computer security venues including IEEE S&P, ACM CCS, USENIX Security, NDSS, WWW, RAID, AsiaCCS, and DIMVA.

Research Interests

Juan's research focuses on computer security, including security issues in systems, software, and networks. He designs and implements novel defenses against cybercrime and targeted attacks including defenses against malware and software vulnerabilities. He is also interested on big data analysis for security, program binary analysis, and censorship resistance.

Manuel Hermenegildo

Distinguished Professor

Manuel Hermenegildo received his Ph.D. degree in Computer Science and Engineering from the University of Texas at Austin, USA, in 1986. He joined the Institute on January 1, 2007 as its founding Scientific Director, continuing in this role until May 2017. He is currently Distinguished Professor at the Institute and also a Full Prof. of Computer Science at the Tech. U. of Madrid, UPM. Previously to joining IMDEA Software, he held the P. of Asturias Endowed Chair in Information Science and Technology at the U. of New Mexico, USA. He was also 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 the president of the Scientific Board of INRIA, member of the Scientific Advisory Board of Dagstuhl, vice-President of Informatics Europe, and member of the Steering Board of EIT Digital, among others. He was also the founding director of the Spanish node of EIT Digital. He has published more than 200 refereed scientific papers and monographs and has given numerous keynotes and invited talks in major conferences. He has also been coordinator and/or principal investigator of many international and national projects, area editor of several journals, and chair and PC member of numerous conferences. He served as General Director for the Spanish national research funding agency, as well as a member of the European Union's high-level advisory boards in information technology (ISTAG, CREST), the board of directors and the scientific board of the Spanish Scientific Research Council (CSIC) and of the Center for Industrial and Technological Development (CDTI), among other national and international duties.

Research Interests

His areas of interest include global program analysis, optimization, verification, and debugging (including resources such as energy and other non-functional properties); abstract interpretation; partial evaluation; parallelism and parallelizing compilers; constraint/logic/functional programming language design and implementation; abstract machines; automatic program documentation; and sequential and parallel computer architecture.

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 has published extensively in programming languages, security, privacy, and cryptography, and was awarded the Best Paper Awards at CRYPTO 2011, PPoPP 2013, and FSE 2016.

He was an invited speaker at numerous venues, including CAV 2016, CSF 2014, ESORICS 2012, ETAPS 2013, EUROCRYPT 2017, IJCAR 2016. 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 is a member of the editorial board of the Journal of Automated Reasoning and of the Journal of Computer Security.

Research Interests

Gilles' research is currently 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.

Juan José Moreno-Navarro

Research Professor, on leave

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 on leave from the Institute. 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. He also coordinated

the Spanish Turing Year and was general chair of the Spanish Conference of Informatics 2013. He is currently an MP in the Regional Government.

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, bibliometrics, 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 chaired the program committee of several international conferences and been a member of the program committee of about 60 others. He has also been in 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 articles which have over 2000 citations.

Research Interests

His research interests focus on program specialization, constraint logic programming, rewrite systems, static analysis of software including analysis of energy consumption and other resource properties of programs, automatic software verification, temporal logics, and semantics-based emulation of languages and systems, and has participated in and led a number of national and European research projects on these topics.

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 Spanish Council for Scientific Research (CSIC) in 2009. In 2013, he was promoted to Associate Professor at the IMDEA Software Institute.

César holds a degree in Ingeniería de Telecomunicación (MSEE) from the Technical University of Madrid (UPM), Spain, granted in 1998. Funded by a Fellowship from La Caixa, he moved to Stanford University, USA, receiving an 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, and he enjoyed a Juan De La Cierva Fellowship between 2008 and 2009.

Research Interests

César's general research interests are the applications of logic, games and automata theory for the development, the understanding, and the verification of computational artifacts. In particular, César's main line of research is the use of formal methods for reactive systems with emphasis on concurrent, embedded and distributed systems. His foundational research includes the temporal verification of concurrent datatypes and distributed systems, runtime verification and applications, and rich specification languages for modern complex software.

Pierre Ganty
Associate Research Professor

Pierre holds a joint Ph.D. degree in Computer Science from the University of Brussels, Belgium and from the University of Genova, Italy that he obtained late 2007. After his Ph.D., Pierre did a nearly two-year postdoc at the University of California, Los Angeles. Pierre joined the IMDEA Software institute in the Fall 2009 as a tenure-track assistant research professor. He was granted tenure and promoted to associate research professor in December 2015. Currently he is supervising two Ph.D. students.

Research Interests
Pierre is interested in automated verification whose goal is to prove the absence of errors in computing systems in a fully automated way. Pierre focuses on systems with infinitely many states in particular concurrent models computation with arbitrarily many agents like population protocols or crowds of processes interacting through a shared register. Pierre is also interested in analysis techniques that are not exhaustive (can find errors but not prove their absence) or not precise (can prove the absence of errors but might report false alarms). 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 Ph.D. in Computer Science from Carnegie Mellon University, and held postdoctoral research positions at Harvard University and Microsoft Research in Cambridge, before joining IMDEA in 2009. He is a recipient of Ramon y Cajal award in 2010, and an ERC consolidator grant in 2016.

Research Interests
Aleks' research focus is on developing type-theoretic ideas on how we should develop and structure mathematical proofs about properties of programs, especially programs utilizing shared-memory concurrency. Structuring proofs builds on the philosophy of structured programming, to identify linguistic concepts that are frequently used in the practice of formal proving, but are arguably harmful. Such concepts should be replaced by better ones that provide proofs with more structure, and improve on the proof's conciseness, readability, development effort and maintainability, just like structured programming improved the very same aspects of programming. Ultimately, these ideas will enable software development practice where verifying that one's programs works correctly will be a simple, natural, and expected process.

Alexey Gotsman
Associate Research Professor

Alexey Gotsman received his Ph.D. degree in Computer Science from University of Cambridge, UK in 2009. 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. He is a recipient of a Ramon y Cajal fellowship, and an ERC Starting Grant in 2016.

Research Interests
Alexey's research interests are in programming models and methods and tools for developing correct concurrent and distributed software.

Boris Köpf
Associate 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 an M.Sc. He is an alumnus of the German National Academic Foundation, holds a Ramón y Cajal fellowship, and is leading a Spanish national project (DEDETIS).

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.

Dario Fiore
Assistant Research Professor

Dario Fiore 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 Ph.D., he was also a visiting student at the IBM T.J. Watson research center and the New York University (USA). He is the recipient of a Juan de la Cierva Incorporacíon fellowship awarded in 2015.

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 IMDEA Software Institute in December 2014 as an assistant research professor, she has been 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. On May 28, 2008 he obtained a Tenured Researcher position at the Spanish National Research Council (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 more than 60 refereed scientific papers, many of them at conferences and journals of high or very high impact. He served as the local principal investigator of the European projects ES_PASS "Embedded Software Product-based ASSurance," and the FP7 FET ENTRA "Whole-Systems Energy Transparency." He has also participated as a researcher in many other international, national, and regional projects.

Research Interests
His areas of interest include energy-aware software development; multi-language analysis, verification, debugging and optimization of non-functional properties, focusing on resources (energy, execution time, user defined), determinism, non-failure, etc.; automatic static profiling of resources; abstract interpretation; low energy and highly parallel computing in different application domains (Internet of Things, Healthcare, Big Data, and HPC); resource-aware program synthesis; automatic control of resources in parallel and distributed computing; tree automata; constraint and logic programming.

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.

Research Interests
Jose's past work 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. His current research interests include the design of multiparadigm languages (declarative, imperative) based on a constraint/logic programming kernel; abstract machines, program optimizations, and native code generation; and program analysis, abstract interpretation, and static and dynamic verification.

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 Díaz, received the ERCIM WG Security and Trust Management Best Ph.D. Thesis Award. During her Ph.D., 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 a Researcher.

Research Interests

Carmela's main research interests revolve around the design of privacy-preserving technologies in the digital word. Her latest research focuses on improving the level of privacy offered by decentralized systems such as those based on block chains, and on finding solutions to enable safe sharing of sensitive data, such as genetic information. She also performs research on the design of better anonymous communications systems and on the design and evaluation of location privacy-preserving mechanisms.

postdoctoral researchers

Guillermo Vigueras
Postdoctoral researcher

Guillermo Vigueras joined IMDEA Software Institute as a postdoctoral researcher in November 2013. He received his Ph.D. degree in Computer Science from University of Valencia (Spain). During his Ph.D. 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 the 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 electromechanical 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

Vincent Laporte
Postdoctoral researcher

Vincent Laporte joined the IMDEA Software Institute as a post-doctoral researcher in January 2016. He received his Ph.D. in Computer Science from the University Rennes 1, France, in 2015, under the supervision of Sandrine Blazy and David Pichardie. During his Ph.D., he contributed to the implementation and the formal verification of the Verasco static analyzer.

Research Interests
Vincent is interested in automatic analysis of programs and in the formal verification of such analyses on semantic grounds. More specifically, he focuses on the automatic proof of program equivalence using product programs, the analysis of smart contracts from the Ethereum block-chain, and the compilation of C programs to circuits to use them in cryptographic protocols. Most of the analyses he implements are formally verified using the Coq proof assistant.

Álvaro García Pérez
Postdoctoral researcher

Álvaro García Pérez received is Ph.D. in September 2014, from IMDEA Software Institute and Universidad Politécnica de Madrid. During his Ph.D. his work focused on semantics of programming languages and meta-theory of the lambda calculus. From 2014 to 2016, he was a postdoctoral researcher at Reykjavik University under the supervision of Luca Aceto. During this time, he worked in nominal techniques, process algebras and concurrency theory. He joined IMDEA Software Institute again as a postdoctoral researcher in January 2017, where he works in verification of consensus algorithms and blockchain systems.

Research Interests
Álvaro's research interests range over the topics of concurrent and distributed systems and of semantics of programming languages. During his Ph.D., he has contributed to the study of abstract machines and lambda calculi with explicit substitutions. He has also developed semantic models for call-by-value programming languages. While in Reykjavik University, his focus was on meta-theory of structural operational semantics, where he has applied nominal set theory to develop rule formats for process calculi with binding constructs. Lately, he has contributed to the verification of consensus protocols in the family of the Paxos algorithm, and he is currently working in Byzantine protocols, federated voting and other aspects related to blockchain technology.

Antonio Faonio
Postdoctoral researcher

Antonio received is Ph.D. degree in Computer Science from Sapienza, University of Rome, Rome, Italy where he was adviced by Giuseppe Ateniese. From 2014 to 2017 he was a postdoc researcher at Aarhus University, advised by Jesper Buus Nielsen. Starting from 2017, he is a postdoctoral researcher at IMDEA Software Institute where he works with Dario Fiore on cryptography.

Research Interests
Antonio's interest are in both theoretical and applied cryptography. He worked on leakage-resilient cryptography, tamper-resilient cryptography, theory of interactive proving systems, non-malleability and controlled-malleability, re-randomizable cryptosystems and verifiable mixing networks.

Wouter Lueks
Postdoctoral researcher

Wouter Lueks received his Bachelor and Master's degrees in Mathematics and Computing Science from the University of Groningen, The Netherlands. In 2017, he received a Ph.D. degree in Computer Science from the Radboud University, Nijmegen, The Netherlands where he was advised by Bart Jacobs and Jaap-Henk Hoepman. Starting 2017, Wouter is a postdoctoral researcher at the IMDEA Software Institute where he works with Carmela Troncoso on privacy-enhancing technologies.

Research Interests
Wouter's research interests are privacy and security. He is interested in building secure, practical, and privacy-friendly systems using applied cryptography and statistical techniques.

Ignacio Fábregas
Postdoctoral researcher

Ignacio Fábregas received both, his bachelor degree in Mathematics and Ph.D. in Computer Science, in Universidad Complutense de Madrid (UCM). Starting in 2017 he has joined the IMDEA Software Institute as a post-doctoral researcher, where he works with Aleks Nanevski on the topic of Separation Logics for Concurrency. Before joining IMDEA Software he was a postdoc in Reykjavik University (Iceland), where he worked with Luca Aceto.

Research Interests
His current research interest are concurrency and logics. In particular, he is interested in separation logics, modal logics, category theory for computer science and process semantics.

Avinash Sudhodanan
Postdoctoral researcher

Avinash Sudhodanan joined the IMDEA Software Institute as a postdoctoral researcher in May 2017. Prior to taking up this position, Avinash was pursuing his Ph.D. in Information and Communication Technology from University of Trento, Italy (graduated in April 2017). During his Ph.D., he worked as an Early-Stage Researcher at the Fondazione Bruno Kessler, Italy. He also spent 18 months of his Ph.D. at SAP Labs France, working closely with the product security research team of SAP. Avinash pursued his Bachelors in Computer Science and Engineering (graduated in 2011) and Masters in Cyber Security (graduated in 2013) from Amrita Vishwa Vidyapeetham University, India.

Research Interests
Avinash's research interests primarily lie in the area of Automatic Detection of Security Vulnerabilities in Web Applications. His Ph.D. research has led to the discovery of hundreds of serious security vulnerabilities in prominent web sites. Recently he also started focusing on the Automatic Detection of Potentially Unwanted Programs and Malware.

Pablo Chico de Guzmán
Postdoctoral researcher

Pablo completed his Ph.D. at the Technical University of Madrid, Spain. The focus of his dissertation was on parallel computation and advanced compilation techniques in order to allow more declarative programming techniques. His dissertation was completed while researching at the IMDEA Software Institute. After his dissertation, he has been working in several worldwide leading companies in the field of cloud computing. In particular, he has developed orchestration tools at Docker for three years. Starting in 2017, he is a postdoctoral researcher at the IMDEA Software Institute where he works with César Sánchez on declarative techniques for massive deployments.

Research Interests
Pablo research interests are cloud computing and the development of declarative and easy to use tools for complex orchestration of distributed systems.

Srdjan Matic
Postdoctoral researcher

Srdjan Matic obtained a B.Sc. and an M.Sc. in computer science from the Universita degli Studi di Milano. During his Ph.D. at the Universita degli Studi di Milano, he spent half of his time as a visiting student at the IMDEA Software Institute. He is a postdoctoral researcher at IMDEA Since June 2017.

Research Interests
Srdjan' research main line of research includes privacy and security issues that affect systems and their users. In the past he studied leaks of sensitive information in public cloud services and topological relations among hosts of spamming infrastructures. During his Ph.D. he focused on anonymity networks and specifically on threats to owners of different services that are available in the Tor network.

Yuri Meshman
Postdoctoral researcher

Yuri Meshman obtained an M.Sc. and a Ph.D. at Technion Israel Institute of Technology as well as a BSc in Mathematics and a BSc in Computer Science. During his BSc, he worked in an IBM Research group as a student software developer. During his Ph.D., he participated in the Fender project, an international research collaboration between Technion, Haifa and ETH, Zurich. Since March 2017, he is a postdoctoral researcher at the IMDEA Software Institute.

Research Interests
Yuri's current research interest are developing and verifying programs for systems with relaxed operational semantics.

research
programmers

Anton Trunov
Degree: Engineer – Tomsk State University of Control Systems and Radioelectronics, Russia

Francy Rodríguez
Degree: Ph.D. – Technical University of Madrid (UPM), Spain

visiting and
affiliate faculty

Roberto Giacobazzi
Affiliate Faculty

Anindya Banerjee
Affiliate Faculty

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).

Miriam García
Research Assistant

Degree: M.Sc. 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).

Artem Khyzha
Research Assistant

Degree: M.Sc. in Software and Systems, Technical University of Madrid (UPM), Spain.

Research: Artem is interested in providing mathematical tools for understanding and proving correctness of concurrent algorithms operating on shared memory. His research efforts have focused on designing techniques for proving linearizability of non-blocking algorithms and data structures, and formalising those techniques in program logics.

Nataliia Stulova
Research Assistant

Degree: M.Sc. in Artificial Intelligence, Technical University of Madrid (UPM), Spain.

Research: Assertion languages, their design and use in automatic program documentation, source code specification and instrumentation. Assertion-based run-time software verification and debugging. Combination of static and dynamic program analysis.

Maximiliano Klemen
Research Assistant

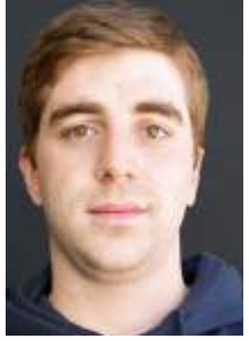
Degree: B.Sc., Universidad Nacional del Comahue (UNCo), Argentina.

Research: Abstract interpretation-based static analysis for inferring energy consumption information about (concurrent) program executions.

Joaquín Arias
Research Assistant

Degree: M.Sc. in Software and Systems, Technical University of Madrid (UPM), Spain.

Research: Design and implementation of advanced programming languages, including logic programming languages featuring constraints and tabling, and their application to reasoning over stream data and abstract interpretation.



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.

Miguel Ambrona
Research Assistant

Degree: M.Sc. in Mathematics for Engineering, Universidad Complutense de Madrid (UCM), Spain.

Research: Computer-aided cryptography with particular emphasis on automatic proofs in the generic group model, improvements on attribute-based encryption and indifferentiability analysis.

Irfan Ul Haq
Research Assistant

Degree: M.Sc. in Information Technology, National University of Sciences and Technology (NUST), Islamabad, Pakistan.

Research: Malware unpacking, binary analysis, web security.

Platon Kotzias
Research Assistant

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

Research: My research interests lie in malware (detection, analysis, classification) and intrusion detection.

Pablo Cañones
Research Assistant

Degree: M.Sc. in Mathematics for Engineering, Universidad Complutense de Madrid (UCM), Spain.

Research: Information theory applied to obtaining security guaranties for cryptographic processes. I focus on the implementation of the algorithms and the hardware architectures they are run into, characterizing possible side channel attacks and obtaining security guaranties of the information leaked.

Paolo Calciati
Research Assistant

Degree: M.Sc. in Informatics, Università della Svizzera Italiana, Lugano, Switzerland.

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

Pepe Vila
Research Assistant

Degree: M.Sc. in Computer Engineering, Escuela de Ingeniería y Arquitectura de la Universidad de Zaragoza (EINA), Spain.

Research: Application security with emphasis on client-side web security, timing attacks against asynchronous systems, and side-channel countermeasures.

Raúl 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. Design of model-driven methodologies for concurrent programming based on shared resources.

Alejandro Aguirre
Research Assistant

Degree: M.Sc. in Informatics, Université Paris Diderot (Paris 7), France.

Research: Formal methods for software verification, with emphasis on the design and implementation of type systems to check relational properties of programs.

Isabel García
Research Assistant

Degree: M.Sc. in Artificial Intelligence, Technical University of Madrid (UPM), Spain.

Research: Abstract interpretation-based static analysis of programs and how it can be applied to semantic code search. Incremental analysis and verification of programs and its applications. Applications of (Constraint) Logic Programming.

Elena Gutierrez
Research Assistant

Degree: Double BS in Computer Science and Mathematics, Universidad Autónoma de Madrid (UAM), Spain.

Research: Formal program verification using Horn clauses: linearisation of constraint logic programs. Applications of automata theory for solving problems in formal languages.

Pedro Valero
Research Assistant

Degree: Double BS in Computer Science and Mathematics, Universidad Autónoma de Madrid (UAM), Spain.

Research: Applications of language's theory into data validation.

Joakim Öhman
Research Assistant

Degree: M.Sc., University of Gothenburg, Sweden.

Research: Formal verification of software and systems. Design and implementation of type theory, especially for concurrent systems.

Jesús Domínguez
Research Assistant

Degree: M.Sc., National Autonomous University of Mexico, México.

Research: Formal verification of software, concurrency, and type theory.

Richard Rivera
Research Assistant

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

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

Bogdan Kulynych
Research Assistant

Degree: M.Sc. in Software and Systems, Tehnical University of Madrid, and BS on Applied Mathematics, National University of Kyiv-Mohyla Academy, Ukraine.

Research: Design and implementation of privacy-preserving systems. Private and anonymous communication.

Umer Liqat
Research Assistant

Degree: M.Sc. in Computational Logic, 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.

intern staff

Intern	Period	Nationality
Sergio Delgado	09/16-06/17	Spain
Sergio Chica	09/16-06/17	Spain
Silvia Sebastián	09/16-06/17	Spain
Anaïs Querol	09/16-08/17	Spain
Javier Prieto	10/16-07/17	Spain
Chiara Redaelli	10/16-02/17	Italy
Martin Zuber	07/16-01/17	France
Elena Pagnin	02/17-04/17	Italy
Borja de Regil	10/16-12/17	Spain
Sergio Valverde	02/17-12/17	Spain
María del Carmen Sánchez	02/17-12/17	Spain
Arianna Blasi	03/17-12/17	Italy
Luis Miguel Danielsson	05/17-12/17	Spain
Álvaro Feal	07/17-12/17	Spain
Guillermo Paredes	09/17-12/17	Spain
Jose Carlos Garde	09/17-12/17	Spain
Roberto Fernández	09/17-12/17	Spain
Amir Goharshady	09/17-12/17	Iran
David Alejandro Lilue	11/17-12/17	Venezuela

project and technology transfer staff

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.

Juan José Collazo
Project Manager

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

Silvia Díaz-Plaza
Project Assistant, N-GREENS

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

Jesús Contreras
EIT Digital Spain Node Director

Degree: MBA – CEREM and Ph.D. in CS, Technical University of Madrid (UPM), Spain.

Francisco Ibáñez
Business Developer
EIT Digital

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

Susana Negrete
Doctoral Training Center Lead
EIT Digital

Degree: Ph.D. in Fungal Genetics and Genetic Engineering, Imperial College, London.

Javier Benito
Business Developer
EIT Digital

Degree: MBA, ESEUNE & Ph.D. in Industrial Organization Engineering, University of the Basque Country, Spain.

Pedro Sánchez
Business Developer Digital

Degree: Technical Degree, Mechanics and Industrial Automation, Lycée technologique du Rempart, Marseille, France.

Carlos Rubal
Business Developer
EIT Digital

Degree: M.Sc. in Management, Northwestern University, USA.

Álvaro de la Cruz
Communications Lead
EIT Digital

Degree: BA in Political Science, UCM, Spain, Certificate of European Policy Studies, Sciences Po Strasbourg, France.

Andrea Iannetta
Administrative Assistant
EIT Digital

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

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: M.Sc. Elec. & Computer Eng., Technical University of Madrid (UPM), Spain.

Juan Céspedes
Network and Systems Engineer

Degree: M.Sc. 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: B.Sc. 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.

research projects and contracts

annual report 2017

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 2017, the Institute participated in a total of 29 funded research projects and contracts, many of which (11, or 38%) involve collaboration with industry and five of them have direct industrial funding. Of these 29 projects, 13 come from international sources (11 funded by the European Union, one by the ONR-US agency, and one by Google), 12 have a national source, and funds for 4 come from regional sources, either through competitive calls or via contracts with companies. 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 2012-2017 (and a representation of the funds already awarded for 2018) is shown in Figure 5.2. The amount of external funding for 2017 has risen to 2.6M€, the highest the Institute has achieved in its history, with the percentage of external funding for research and innovation w.r.t. the total Institute budget reaching a 46%. The current forecast for 2018 places the external funding below this all-time maximum, in a point close to 2.4M€. This figure is of course dependent on the outcome of the recently submitted project proposals (and on those to be submitted and decided upon within the rest of the year), which typically raises this estimation.

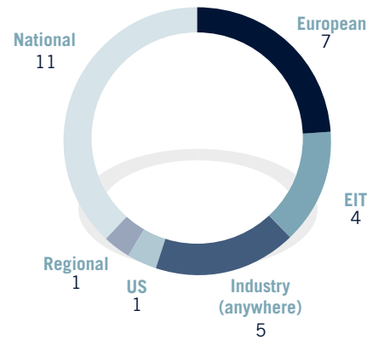


Figure 5.1. Projects by origin of funding.

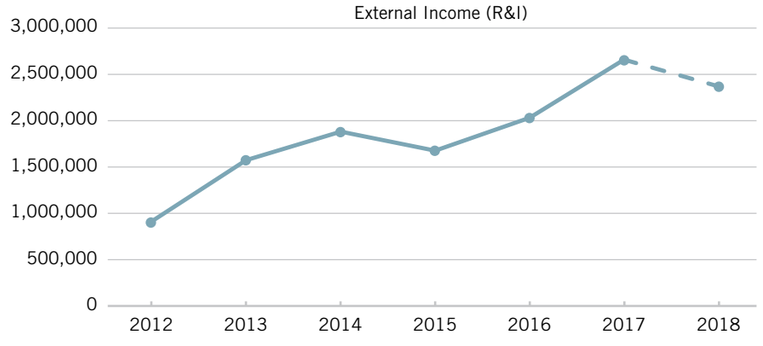


Figure 5.2. Evolution in external funding since 2012.

5.1. Projects Running in 2017

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.

EIT Digital Spain
EIT Digital Spain: Coordination and Joint Activities

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2015-2017
Principal Investigator: Res. Prof. Manuel Hermenegildo

As mentioned in Section 2.3, EIT Digital is the Knowledge and Innovation Community (KIC) in the ICT sector of the European Institute of Innovation and Technology. The Spanish members of EIT Digital at the end of 2017 are Atos, Ferrovial, Fundación General de la UPM, IMDEA Software, Indra, Nokia-Spain, Telefónica, and UPM. The duties of IMDEA Software, as project beneficiary, focus on boosting the network in collaboration with members of the node with a twofold objective: on the one hand, to improve knowledge of the KIC possibilities in order to take maximal profit from the innovation program, and on the other hand to spread the activities of the KIC in the National ICT sector at all levels: large companies, SMEs, entrepreneurs, students, academia and researchers.

N-GREENS

Next-Generation Energy-Efficient Secure Software

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

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, cyberphysical 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.

StrongSoft

Sound Technologies for Reliable, Open, New Generation Software

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2013–2017
Principal Investigator: Res. Prof. Gilles Barthe

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

e-TUR2020

e-TUR2020. TUrismo & Retail

Funding: Spanish Ministry of Economy, Industry 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: 2012-2017
General Coordinator: Res. Prof. Manuel Hermenegildo

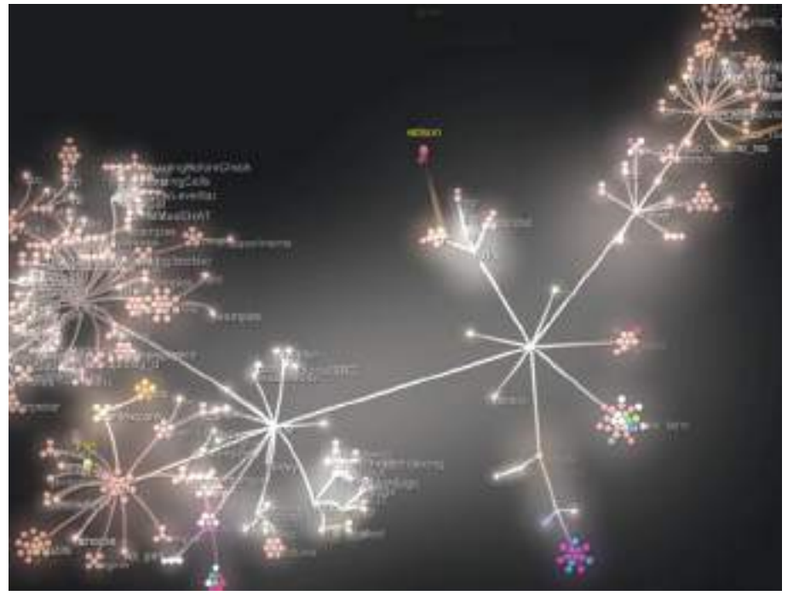
AMAROUT-II Europe is a PEOPLE-COFUND Marie Curie Action which continues the AMAROUT action sharing with it the objectives of fostering and consolidating the European Research Area by attracting top research talent to Europe and, in particular, to the region of Madrid. As in the previous AMAROUT program, "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 5 years, more than 150 experienced researchers to carry out research projects within the IMDEA network of research Institutes. 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.

EUIN Grants

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2017 – 2018

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 two of these grants to support the submission of two research proposals to the European Research Council (for Starting Grant, made by Dario Fiore and Advanced Grant, made by Roberto Giacobazzi) in 2017.



EIT Digital CLC
Co-Location Center

The IMDEA Software Institute hosts the Co-Location Center (CLC) of the Madrid Node of EIT Digital. The Madrid CLC is the central place for organizing and implementing EIT Digital activities in Spain, and the main meeting point for the members of the node (see Section 2.3).

EIT Digital Accelerator

The Digital Business Developers (BDs) are part of the EIT Digital BD 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 2017 the business acceleration activities of the Madrid Node, led by the IMDEA Software Institute, have been expanded to four people with a new additional expert establishing relationships with the Spanish corporate and entrepreneurship ecosystems.

EIT Digital Higher Education Schools

During 2017, the Spanish Node consolidated the EIT Digital Doctoral and the Master School. Several entrepreneurship courses and students working on a daily basis turned the Co-Location Center into a vibrant place for innovation.

ANTIFRAUD
Online Banking Anti-Fraud Monitoring

Funding: EIT Digital
Duration: 2017
General Coordinator: Assoc. Res. Prof. Juan Caballero

The “Online banking anti-fraud monitoring” innovation activity is one of three innovation activities of the Digital Finance Action Line of EIT Digital in 2017. Digital Finance, also known as “FinTech” focuses on the delivery of innovative financial products and services through digital technology, with the objective of making financial systems more reliable, transparent, and customer friendly, improving thus the banking experience for the society and reducing the dependency of banks on central infrastructures.

NEXTLEAP
NEXt Generation Technosocial and Legal Encryption Access and Privacy

Funding: European Union – H2020 Framework Program
Duration: 2016-2018
Principal Investigators: Asst. Res. Prof. Dario Fiore – Res. Carmela Troncoso

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 long term 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, Industry and Competitiveness
Duration: 2016-2019
Principal Investigators: Assoc. Res. Prof. Manuel Carro – Res. Prof. Manuel Hermenegildo

The TRACES project revolves around 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 (and maybe 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

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2016-2018
Principal Investigators: Assoc. Res. Prof. Juan Caballero – Assoc. 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.

RISCO

Rigorous Technologies for the Analysis and Verification of Sophisticated Concurrent Software

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2016-2018
Principal Investigators: Assoc. Res. Prof. Pierre Ganty – Assoc. 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 for the 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 the complexity of the verification problems for the above modern concurrent and distributed computational models, and 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.

AxE Javascript

Auditable E-voting using Javascript

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2016-2018
Principal Investigator: Res. Prof. Gilles Barthe

The AxE Javascript Project aims to bring a solution to confidence problems in the field of security in electronic voting systems through the development of an e-voting software with the highest possible correctness and security properties. Identifying and defining properties for security in e-voting systems and developing and implementing new methods providing real evidence of correctness and security in e-voting systems, AxE Javascript project aims to develop a solution for e-voting including the highest actually possible guarantees regarding code correctness and security. This will allow a significant improvement in the transparency of e-voting systems used by electoral organizations.

DataMantium

Computación y comunicaciones seguras en la nube para entornos hostiles

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2016-2018
Principal Investigators: Asst. Res. Prof. Dario Fiore – Res. Carmela Troncoso

The goal of DataMantium project is to develop security mechanisms to protect the integrity and privacy in users data and processes in untrusted cloud scenarios. The results of the project totally aim at issues specially relevant in cybersecurity and digital trust, such as cryptography, to protect the information's confidentiality and integrity and the development of communication technologies in private and secure networks.

RiskIoT

Sistema de Monitorización Proactiva en Infraestructuras Críticas Basado en Tecnologías IoT

Funding: Regional Government of Madrid
Duration: 2017-2018
Principal Investigator: Asst. Res. Prof. Alessandra Gorla

The possibility of almost instantaneously sharing data in the IoT world gives unprecedented power and, at the same time, poses great security and access control threats. It is therefore necessary to furnish new means to securely exchange data and events between the virtual and physical world. RiskIoT addresses this problem for the case of seaport environments, a critical infrastructure where a huge number of objects, companies, cameras, security sensors, persons, etc. have to safely interact and exchange information while ensuring compliance with existing legal regulations, including data provenance and privacy. The goal of RiskIoT is to provide a security middleware to make this information transmission possible, without interruptions, and abiding by the applicable laws.

Ciber4.0

Plataforma de Ciberseguridad Interoperable para Entornos IoT en la Industria 4.0

Funding: Regional Government of Madrid
Duration: 2017-2018
Principal Investigator: Assoc. Res. Prof. Juan Caballero

Internet of Things (IoT) make it possible the interconnection of many different "things" (devices, networks, systems, ...). That makes it possible a leap forward in productivity in industry. However, this brings about interoperativity and vulnerability problems that can be (and are) exploited by cybercriminals. In order to provide protection against these issues, Ciber4.0 is developing an interoperable framework that will analyze data traffic in IoT environments regardless of the protocols used or which devices are interconnected, with the aim of detecting possible security threats.

Europa Excelencia

Funding: Spanish Ministry of Economy, Industry and Competitiveness
Duration: 2016-2017

The *Europa Excelencia* grants, funded by the MINECO, support proposals submitted to ERC Starting and Consolidator Grants from Spanish research centers which were ranked with A, but not funded due to budget constraints. IMDEA Software has obtained two of these grants to support the development of some tasks included in the research proposals submitted to the European Research Council (for Consolidator Grants and Starting Grants, by Aleksandar Nanevski and Alexey Gotsman) in 2015.

RACOON

A Rigorous Approach to Consistency in Cloud Databases

Funding: European Union, European Research Council – H2020 Framework Program
Duration: 2017-2021
Principal Investigator: Assoc. Res. Prof. Alexey Gotsman

The goal of this project is to develop a synergy of novel reasoning methods, static analysis tools, and database implementation techniques that maximally exploit parallelism inside cloud databases, while enabling application programmers to ensure correctness. We intend to achieve this by first developing methods for reasoning formally about how weakening the consistency guarantees provided by cloud databases affects application correctness and the parallelism allowed inside the databases. This will build on techniques from the areas of programming languages and software verification. The resulting theory will then serve as a basis for practical implementation techniques and tools that harness database parallelism, but only to the extent such that its side effects do not compromise application correctness.

Mathador

Type and Proof Structures for Concurrent Software Verification

Funding: European Union, European Research Council – H2020 Framework Program
Duration: 2017-2022
Principal Investigator: Assoc. Res. Prof. Aleksandar Nanevski

The grand challenge of this project is to remove existing limitations which make proofs generated with proof assistants unmanageable by humans, and to scale dependent types to support the implementation of stateful concurrent programs and their correctness proofs simultaneously. By applying the modularizing power of dependent types to both programs and proofs, the project will obtain novel and scalable foundations for the field of concurrent software verification. Writing mechanized proofs of software, concurrent or otherwise, is generally considered infeasible. But if one chooses the right linguistic abstractions to express the proofs, we argue that it does not have to be so. This observation is supported by our encouraging preliminary results. The project will design further novel linguistic abstractions that facilitate engineering of practically feasible formal proofs, and experimentally evaluate them by mechanically verifying extensive concurrent programs drawn from realistic applications, such as concurrent garbage collectors, OS kernels, and popular open-source concurrent libraries.

ELASTEST

ElasTest: an elastic platform for testing complex distributed large software systems

Funding: European Union – H2020 Framework Program
Duration: 2017-2019
Principal Investigators: Assoc. Res. Prof. César Sánchez – Assoc. Res. Prof. Juan Caballero

This project aims at significantly improving the efficiency and effectiveness of the testing process and, with it, the overall quality of large software systems. For this, we propose to apply the “divide-and-conquer” principle, which is commonly used for architecting complex software, to testing by developing a novel test orchestration theory and toolbox enabling the creation of complex test suites as the composition of simple testing units. This test orchestration mechanism is complemented with a number of tools that include: (1) Capabilities for the instrumentation of the Software under Test enabling to reproduce real-world operational conditions thanks to features such as Packet Loss as a Service, Network Latency as a Service, Failure as a Service, etc.; (2) Reusable testing services solving common testing problems including Browser Automation as a Service, Sensor Emulator as a Service, Monitoring as a Service, Security Check as a Service, Log Ingestion and Analysis as a Service, Cost Modeling as a Service, etc; (3) Cognitive computing and machine learning mechanisms suitable for ingesting large amounts of knowledge (e.g. specifications, logs, software engineering documents, etc.) and capable of using it for generating testing recommendations and answering natural language questions about the testing process. The ElasTest platform thus created shall be released basing on a flexible Free Open Source Software and a community of users, stakeholders and contributors shall be grown around it with the objective of transforming ElasTest into a worldwide reference in the area of large software systems testing and of guaranteeing the long term sustainability of the project generated results.

VEECC

VEECC: Verified and Efficient Elliptic Curve

Funding: Google
Duration: 2016-2017
Principal Investigator: Res. Prof. Gilles Barthe

Within this project IMDEA researchers propose to develop a methodology for building efficient, provably correct, and provably "constant-time" implementations of elliptic curve cryptography. These algorithms will be a key building block for the next generation TLS, and are therefore of utmost relevance for applications that require secure communication and to Google Chrome.

Concretely, IMDEA propose to broaden the scope of computer-aided cryptography to implementations, by taking the following steps: (i) propose a portable assembly language for writing efficient implementations, together with a verification method for proving correctness and a verified compiler; (ii) develop an automated method for proving "constant-time" at the assembly level; (iii) apply our approach and tools to build efficient and verified implementations of elliptic curve arithmetic for NIST P256 and Curve25519, and selected cryptographic constructions based on elliptic curves; (iv) extend the tool and method to vectorized implementations on other platforms. The deliverables of the project include formalizations, tools, and verified and efficient implementations.

NetVote

NetVote

Funding: INDRA
Duration: 2017
Principal Investigator: Res. Carmela Troncoso

Research project funded by INDRA aimed to study and improve the voting on line protocol developed by the company in terms of security (vulnerability under attacks, security properties supported,...) and reliability (is voter anonymity guaranteed in all assumptions?, related trust assumptions, coercion resistance, etc.)

5.2 Projects to Start in 2018

NEC Industrial Research Grant

Secure Cloud Storage with Controlled Computation

Funding: NEC
Duration: 2018
Principal Investigator: Asst. Res. Prof. Dario Fiore

IMDEA researchers have started a research program funded by NEC to investigate in two major directions. On the one side, they plan to devise cryptographic schemes that reconciliate user privacy with the great computational power of cloud providers that is key in computations over large data sets. On the other hand, they will investigate what benefits can secure hardware provide in this context and how secure hardware can improve the provisions of cryptographic protocols for cloud storage.

5.3 Joint R+D Units

Telefónica I+D

As previously mentioned, Telefónica Digital and the Institute established during 2013 a *Joint Research Unit* (JRU) within their more global strategic partnership. This unit made it possible the joint participation of Telefónica and IMDEA Software in the FI-CORE EU Project and it currently channels the collaboration of researchers and students hired at IMDEA in EIT Digital activities where Telefónica takes also part.

5.4 Fellowships

1. *Juan de la Cierva Postdoc Incorporación grant*, Spanish Ministry of Economy, Industry and Competitiveness, awarded in 2015 and ending in 2017 (**Dario Fiore**).

2. *Ramón y Cajal grant*, Spanish Ministry of Economy, Industry and Competitiveness, awarded in 2016 and ending in 2021 (**Alexey Gotsman**).

3. *Ramón y Cajal grant*, Spanish Ministry of Economy, Industry and Competitiveness, awarded in 2015 and ending in 2020 (**Boris Köpf**).

4. *Estabilización Doctores I3 grant*, Spanish Ministry of Economy, Industry and Competitiveness, awarded in 2017 and ending in 2019 (**Aleks Nanevski**).

5. *Marie Curie AMAROUT II Incoming Fellowships (5)*, European Union – 7 Framework Program, awarded in 2012 and active in 2017 (**Vincent Laporte**, **Yuri Meshman**, **Álvaro García**, **Antonio Faonio** and **Matthieu Perrin**).

6. *FPI Doctoral Grant*, Spanish Ministry of Economy, Industry and Competitiveness, active in 2017 (**Miriam García**).

7. *Atracción de talento Grants*, Madrid Regional Government, awarded in 2016, and ending in 2018 (**Roberto Giacobazzi**).

8. *Predoctoral Grants*, Madrid Regional Government, awarded in 2016, and ending in 2018 (**Isabel García**).

9. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, awarded in 2016 and ending in 2020 (**Elena Gutierrez**).

10. *FPU Doctoral Grant*, Spanish Ministry of Education, Culture and Sports, awarded in 2017 and ending in 2020 (**Isabel García**).

Comunidad de Madrid · Unión Europea · Gobierno de España Ministerio de Educación, Cultura y Deporte · Gobierno de España Ministerio de Economía, Industria y Competitividad

dissemination of results

annual report 2017

6.1 Publications

The vast majority of the research of the Institute is published at highly-ranked conferences and journals. In line with what is common in Computer Science, and unlike what happens in other disciplines, conferences are often preferred to journals for a variety of reasons. Therefore, most of our researchers target them primarily to present bleeding-edge work, and submit to journals only archival papers after they have been presented at the leading conferences of their fields.

In addition to peer-reviewed papers, we list in this section conference proceedings edited by our researchers, articles in books, and theses (at the levels of Bachelor, Master, and PhD).

6.1.1 Refereed Publications

Journals

1. Alejandro Aguirre, Gilles Barthe, Marco Gaboardi, Deepak Garg, Pierre-Yves Strub. *A Relational Logic for Higher-Order Programs*. PACMPL (ICFP), Vol. 1, pages 1–29, ACM, August 2017.

2. Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, Jean Karim Zinzindohoue. A Messy State of the Union: Taming the Composite State Machines of TLS. Communications of the ACM 60(2), pages 99-107, 2017.

3. Dario Catalano, Dario Fiore, Rosario Gennaro. *A Certificateless Approach to Onion Routing*. International Journal of Information Security, Vol. 16, Num. 3, pages 327–343, Springer, June 2017.

4. Véronique Cortier, Constantin Catalin Dragan, François Dupressoir, Benedikt Schmidt, Pierre-Yves Strub, Bogdan Warinschi. Machine-Checked Proofs of Privacy for Electronic Voting Protocols. IEEE Symposium on Security and Privacy 2017, pages 993-1008.

5. Antoine Durand-Gasselin, Javier Esparza, Pierre Ganty, Rupak Majumdar. *Model Checking Parametrized Asynchronous Shared-Memory Systems*. Formal Methods in System Design, Vol. 50, Num. 2-3, pages 140–167, June 2017.

6. Javier Esparza, Pierre Ganty, Jérôme Leroux, Rupak Majumdar. *Verification of Population Protocols*. Acta Informatica, Vol. 54, Num. 2, pages 191–215, March 2017.

7. Dario Fiore, María Isabel González Vasco, Claudio Soriente. *Partitioned Group Password-Based Authenticated Key Exchange*. The Computer Journal, Vol. 60, Num. 12, pages 1912–1922, 2017.

8. Pierre Ganty, Radu Iosif, Filip Konečný. *Underapproximation of Procedure Summaries for Integer Programs*. International Journal on Software Tools for Technology Transfer (STTT), Vol. 19, Num. 5, pages 565–584, October 2017.

9. Roberto Giacobazzi, Isabella Mastroeni, Mila Dalla Preda. *Maximal Incompleteness as Obfuscation Potency*. Formal Aspects of Computing, Vol. 29, Num. 1, pages 3–31, January 2017.

10. Damien Imbs, Achour Mostéfaoui, Matthieu Perrin, Michel Raynal. Which Broadcast Abstraction Captures k-Set Agreement? DISC 2017, 27:1-27:16.

11. Bishoksan Kafle, John P. Gallagher. *Horn Clause Verification with Convex Polyhedral Abstraction and Tree Automata-based Refinement*. Computer Languages, Systems & Structures, Vol. 47, pages 2–18, 2017.

12. Bishoksan Kafle, John P. Gallagher. *Constraint Specialisation in Horn Clause Verification*. Science of Computer Programming, Vol. 137, pages 125–140, 2017.

13. U. Liqat, Z. Bankovi€, P. López-García, M. V. Hermenegildo. *An Evolutionary Scheduling Approach for Trading-off Accuracy vs. Verifiable Energy in Multicore Processors*. Logic Journal of the IGPL, Vol. 25, Num. 6, pages 1006–1019, Oxford Academic Press, December 2017.

14. Apostolos Pyrgelis, Carmela Troncoso, Emiliano De Cristofaro. *What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy*. PoPETs, Vol. 2017, Num. 4, pages 156–176, 2017.

15. Alejandro Sánchez, César Sánchez. *Parametrized Verification Diagrams: Temporal Verification of Symmetric Parametrized Concurrent Systems*. Annals of Mathematics and Artificial Intelligence, Vol. 80, Num. 3–4, pages 249–282, August 2017.

16. Reza Shokri, George Theodorakopoulos, Carmela Troncoso. *Privacy Games Along Location Traces: A Game-Theoretic Framework for Optimizing Location Privacy*. ACM Trans. Priv. Secur., Vol. 19, Num. 4, pages 1–31, 2017.

17. Carmela Troncoso, George Danezis, Marios Isaakidis, Harry Halpin. *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments*. PoPETs, Vol. 2017, Num. 4, pages 404–426, 2017.

Conferences

1. Luca Aceto, Ignacio Fábregas, Álvaro García-Pérez, Anna Ingólfsdóttir, Yolanda Ortega-Mallén. *Rule Formats for Nominal Process Calculi*. 28th International Conference on Concurrency Theory, CONCUR 2017, September 5-8, 2017, Berlin, Germany, LIPIcs, Vol. 85, pages 1–16, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

2. Miguel Ambrona, Gilles Barthe, Romain Gay, Hoeteck Wee. *Attribute-Based Encryption in the Generic Group Model: Automated Proofs and New Constructions*. Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30-November 3, 2017, pages 647–664, ACM, 2017.

3. Miguel Ambrona, Gilles Barthe, Benedikt Schmidt. *Generic Transformations of Predicate Encodings: Constructions and Applications*. Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 10401, pages 36–66, Springer, 2017.

4. Vitalii Avdiienko, Konstantin Kuznetsov, Alessandra Gorla, Andreas Zeller, Steven Arzt, Siegfried Rasthofer, Eric Bodden. *AppMining*. Software Engineering 2017, LNI, Vol. P-267, pages 113–114, GI, February 2017.

5. Vitalii Avdiienko, Konstantin Kuznetsov, Isabelle Rommelfanger, Andreas Rau, Alessandra Gorla, Andreas Zeller. *Detecting Behavior Anomalies in Graphical User Interfaces*. Proc. of the 39th International Conference on Software Engineering (ICSE 2017), pages 201–203, IEEE Computer Society, May 2017.

6. José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Arthur Blot, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Hugo Pacheco, Benedikt Schmidt, Pierre-Yves Strub. *Jasmin: High-Assurance and High-Speed Cryptography*. Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30-November 3, 2017, pages 1807–1823, ACM, 2017.

7. José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte, Vitor Pereira. *A Fast and Verified Software Stack for Secure Function Evaluation*. Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30-November 3, 2017, pages 1989–2006, ACM, 2017.

8. Manuel Barbosa, Dario Catalano, Dario Fiore. *Labeled Homomorphic Encryption: Scalable and Privacy-Preserving Processing of Outsourced Data*. Proc. of the 22nd European Symposium on Research in Computer Security (ESORICS 2017), LNCS, Vol. 10492, pages 146–166, Springer, September 2017.

9. Gilles Barthe, Sandrine Blazy, Vincent Laporte, David Pichardie, Alix Trieu. *Verified Translation-Validation of Static Analyses*. 30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, USA, August 21-25, 2017, pages 405–419, IEEE Computer Society, 2017.

10. Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, Pierre-Yves Strub. *Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model*. Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 10210, pages 535–566, 2017.

11. Gilles Barthe, Thomas Espitau, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub. *Proving Uniformity and Independence by Self-Composition and Coupling*. LPAR-21, 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning, Maun, Botswana, 7-12th May 2017, EPiC Series, Vol. 46, pages 385–403, EasyChair, 2017.

12. Gilles Barthe, Thomas Espitau, Justin Hsu, Tetsuya Sato, Pierre-Yves Strub. **-Liftings for Differential Privacy*. 44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland, LIPIcs, Vol. 80, pages 1–12, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

13. Gilles Barthe, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub. *Coupling Proofs are Probabilistic Product Programs*. Proc. of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017, pages 161–174, ACM, 2017.

14. Paolo Calciati, Alessandra Gorla. *How do Apps Evolve in their Permission Requests?: a Preliminary Study*. Proc. of the 14th International Conference on Mining Software Repositories (MSR 2017), pages 37–41, IEEE Computer Society, May 2017.

15. Matteo Campanelli, Rosario Gennaro, Steven Goldfeder, Luca Nizzardo. *Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for Services.* ACM CCS 2017 – 24rd ACM Conference on Computer and Communication Security, pages 229–243, 2017.

16. Pablo Cañones, Boris Köpf, Jan Reineke. *Security Analysis of Cache Replacement Polices*. Proc. 6th Conference on Principles of Security and Trust (POST '17), Springer, 2017.

17. Andrea Cerone, Alexey Gotsman, Hongseok Yang. *Algebraic Laws for Weak Consistency*. CONCUR'17: International Conference on Concurrency Theory, LIPICS, Vol. 85, pages 1–18, Dagstuhl, 2017.

18. Ezgi Çiçek, Gilles Barthe, Marco Gaboardi, Deepak Garg, Jan Hoffmann. *Relational Cost Analysis*. Proc. of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017, pages 316–329, ACM, 2017.

19. Pedro R. D'Argenio, Gilles Barthe, Sebastian Biewer, Bernd Finkbeiner, Holger Hermanns. *Is Your Software on Dope? - Formal Analysis of Surreptitiously "Enhanced" Programs*. Programming Languages and Systems - 26th European Symposium on Programming, ESOP 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings, Lecture Notes in Computer Science, Vol. 10201, pages 83–110, 2017.

20. Germán Andrés Delbianco, Ilya Sergey, Aleksandar Nanevski, Anindya Banerjee. *Concurrent Data Structures Linked in Time*. European Conference on Object-Oriented Programming (ECOOP), pages 1–30, 2017.

21. Yevgeniy Dodis, Dario Fiore, *Unilaterally-Authenticated Key Exchange.* Financial Cryptography and Data Security 2017, Proceedings, LNCS, Springer, 2017.

22. Goran Doychev, Boris Köpf. *Rigorous Analysis of Software Countermeasures Against Cache Attacks*. 38th ACM SIGPLAN Conference on Programming Language Design and Implementations (PLDI), ACM, 2017.

23. Marina Egea, Carolina Dania. *SQL-PL4OCL: An Automatic Code Generator from OCL to SQL Procedural Language*. 20th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, TX, USA, September 17-22, 2017.

24. Alessio Gambi, Alessandra Gorla, Andreas Zeller. *O!Snap: Cost-Efficient Testing in the Cloud*. Proc. of the IEEE International Conference on Software Testing, Verification and Validation (ICST 2017), pages 454–459, IEEE Computer Society, March 2017.

25. Graeme Gange, Pierre Ganty, Peter J. Stuckey. *Fixing the State Budget: Approximation of Regular Languages with Small DFAs*. Proc. of the 15th International Symposium on Automated Technology for Verification and Analysis (ATVA 2017), LNCS, Vol. 10482, pages 67–83, Springer, October 2017.

26. Pierre Ganty, Boris Köpf, Pedro Valero. *A Language-Theoretic View on Network Protocols*. Proc. of the 15th International Symposium on Automated Technology for Verification and Analysis (ATVA 2017), LNCS, Vol. 10482, pages 363–379, Springer, October 2017.

27. Pierre Ganty, Elena Gutiérrez. *Parikh Image of Pushdown Automata*. Proc. of the 21st International Symposium on Fundamentals of Computation Theory (FCT 2017), LNCS, Vol. 10472, pages 271–283, Springer, September 2017.

28. Alexey Gotsman, Sebastian Burckhardt. *Consistency Models with Global Operation Sequencing and their Composition*. DISC'17: International Symposium on Distributed Computing, LIPICS, Vol. 91, pages 1–16, Dagstuhl, 2017.

29. Oliver Kennedy, D. Richard Hipp, Stratos Idreos, Amélie Marian, Arnab Nandi, Carmela Troncoso, Eugene Wu. *Small Data*. Proc. of the 33rd IEEE International Conference on Data Engineering (ICDE 2017), pages 1475–1476, IEEE Computer Society, April 2017.

30. Artem Khyzha, Mike Dodds, Alexey Gotsman, Matthew Parkinson. *Proving Linearizability Using Partial Orders*. ESOP'17: European Symposium on Programming, Uppsala, Sweden, LNCS, Vol. 10201, pages 639–667, Springer, 2017.

31. Chaz Lever, Platon Kotzias, Davide Balzarotti, Juan Caballero, Manos Antonakakis. *A Lustrum of Malware Network Communication: Evolution and Insights*. Proc. of the 38th IEEE Symposium on Security and Privacy, May 2017.

32. Heiko Mantel, Alexandra Weber, Boris Köpf. *A Systematic Study of Cache Side Channels across AES Implementations*. Proc. 9th International Symposium on Engineering Secure Software and Systems (ESSoS '17), Springer, 2017.

33. Srdjan Matic, Carmela Troncoso, Juan Caballero. *Dissecting Tor Bridges: a Security Evaluation of their Private and Public Infrastructures*. Proc. of the Network and Distributed System Security Symposium, February 2017.

34. Andreas Metzger, Philipp Leitner, Dragan Ivanovic, Eric Schmieders, Rod Franklin, Manuel Carro, Schahram Dustdar, Klaus Pohl. *Vergleich und Kombination von Techniken des Predictive Business Process Monitoring*. Software Engineering 2017, Fachtagung des GI-Fachbereichs Softwaretechnik, Lecture Notes in Informatics (LNI), Vol. P-267, pages 79–80, February 2017.

35. Martín Ochoa, Sebastian Banescu, Cynthia Disenfeld, Gilles Barthe, Vijay Ganesh. *Reasoning about Probabilistic Defense Mechanisms Against Remote Attacks*. 2017 IEEE European Symposium on Security and Privacy, EuroS&P 2017, Paris, France, April 26-28, 2017, pages 499–513, IEEE, 2017.

36. Simon Oya, Fernando Pérez-González, Carmela Troncoso. *Filter Design for Delay-based Anonymous Communications*. Proc. of the 42nd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2017), pages 2107–2111, IEEE, March 2017.

37. Simon Oya, Carmela Troncoso, Fernando Pérez-González. *Back to the Drawing Board: Revisiting the Design of Optimal Location Privacy-preserving Mechanisms*. Proc. of the ACM Conference on Computer and Communications Security (CCS 2017), pages 1959–1972, ACM, 2017.

38. Pavithra Prabhakar, Miriam García Soto. *Formal Synthesis of Stabilizing Controllers for Switched Systems*. Proc. of the 20th International Conference on Hybrid Systems: Computation and Control, HSCC 2017, Pittsburgh, PA, USA, April 18-20, pages 111–120, 2017.

39. Pepe Vila, Boris Köpf. *Loophole: Timing Attacks on Shared Event Loops in Chrome*. 26th USENIX Security Symposium, USENIX Association, 2017.

40. Carmen Elisabetta Zaira Baltico, Dario Catalano, Dario Fiore, Romain Gay. *Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption*. Advances in Cryptology: Proc. of the 37th Annual Cryptology Conference (CRYPTO 2017), LNCS, Vol. 10401, pages 67–98, Springer, August 2017.

Workshops

1. Gustavo Betarte, Juan Diego Campo, Felipe Gorostiaga, Carlos Luna. *A Certified Reference Validation Mechanism for the Permission Model of Android*. Pre-proceedings of the 27th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'17), October 2017. arXiv:1709.03652.

2. M. V. Hermenegildo, P. López-García, U. Liqat, M. Klemen. *Energy Consumption Analysis and Verification by Transformantion into Horn Clauses and Abstract Interpretation*. 5th International Workshop on Verification and Program Transformation (VPT 2017), Vol. 253, pages 4–6, EPTCS, April 2017. (Abstract of invited talk).

3. Platon Kotzias, Juan Caballero. *An Analysis of Pay-per-Install Economics Using Entity Graphs*. 16th Annual Workshop on the Economics of Information Security, June 2017.

4. U. Liqat, Z. Bankovi€, P. López-García, M. V. Hermenegildo. *Inferring Energy Bounds via Static Program Analysis and Evolutionary Modeling of Basic Blocks*. Pre-proceedings of the 27th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'17), October 2017. arXiv:1601.02800.

5. Simon Oya, Carmela Troncoso, Fernando Pérez-González. *Is Geo-Indistinguishability What You Are Looking for?*. Proc. of the 16th Workshop on Privacy in the Electronic Society (WPES 2017), pages 137–140, ACM, 2017.

6. Nataliia Stulova. *On Improving Run-time Checking in Dynamic Languages*. Technical Communications of the 33rd International Conference on Logic Programming (ICLP 2017), OpenAccess Series in Informatics (OASIcs), Vol. 58, pages 15:1–15:10, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, CP/ICLP/SAT Doctoral Program, August 2017.

7. N. Stulova, J. F. Morales, M. V. Hermenegildo. *Towards Run-time Checks Simplification via Term Hiding (Extended Abstract)*. Technical Communications of the 33rd International Conference on Logic Programming (ICLP 2017), Open Access Series in Informatics (OASIcs), Vol. 58, pages 9:1–9:3, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, August 2017.

8. Salvador Tamarit, Julio Mariño, Guillermo Vigueras, Manuel Carro. *Towards a Semantics-Aware Code Transformation Toolchain for Heterogeneous Systems*. Proc. of "XIV Jornadas sobre Programación y Lenguajes" (PROLE 2016), EPTCS, September 2017.

9. Guillermo Vigueras, Manuel Carro, Salvador Tamarit, Julio Mariño. *Towards Automatic Learning of Heuristics for Mechanical Transformations of Procedural Code*. Proc. of "XIV Jornadas sobre Programación y Lenguajes" (PROLE 2016), EPTCS, September 2017.

6.1.2 Edited Volumes

1. Giorgos Fagas, Luca Gammaitoni, John P. Gallagher, Douglas J. Paul (Eds.). *ICT: Energy Concepts for Energy Efficiency and Sustainability*. 248 pages, InTech Open Access Publishers, March 2017.

2. M. V. Hermenegildo, P. López-García (Eds.). *Logic-Based Program Synthesis and Transformation - 26th International Symposium, LOPSTR 2016, Edinburgh, UK, September 6-8, 2016, Revised Selected Papers*. Lecture Notes in Computer Science, Num. 10184, 330 pages, Springer, July 2017.

6.1.3 Articles in Books and Other Collections

1. Kerstin Eder, John P. Gallagher. *Energy-Aware Software Engineering*. ICT - Energy Concepts for Energy Efficiency and Sustainability, pages 103–127, InTech Open Access Publishers, March 2017.

2. Giorgos Fagas, John P. Gallagher, Luca Gammaitoni, Douglas J. Paul. *Energy Challenges for ICT*. ICT - Energy Concepts for Energy Efficiency and Sustainability, InTech Open Access Publishers, March 2017.

3. Alberto Goffi, Alessandra Gorla, Andrea Mattavelli, Mauro Pezzè. *Intrinsic Redundancy for Reliability and Beyond*. Present and Ulterior Software Engineering, pages 153–171, Springer, 2017.

4. P. López-García, M. V. Hermenegildo, M. Klemen, U. Liqat. *Energy Consumption Analysis and Verification using CiaoPP*. The ALP Newsletter, Vol. 30, Num. 3, The Association for Logic Programming, September 2017.

5. Salvador Tamarit, Guillermo Vigueras, Manuel Carro, Julio Mariño. *Machine Learning-Driven Automatic Program Transformation to Increase Performance in Heterogeneous Architectures*. Tools for High Performance Computing 2016, Springer International Publishing, 2017.

6.1.4 Doctoral, Master and Bachelor Theses

1. German Delbianco. *Hoare-style Reasoning with Higher-order Control: Continuations and Concurrency*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). July 2017. Advisor: Aleks Nanevski (IMDEA Software Institute).

2. Miriam García. *An Algorithmic Approach for Stability Verification of Hybrid Systems*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM), July 2017. Advisor: Pavithra Prabhakar (Kansas State University).

3. Srdjan Matic. *Active Techniques for Revealing and Analyzing the Security of Hidden Servers*. Ph.D. Thesis. Università degli Studi di Milano, February 2017. Advisors: Danilo Bruschi (Università degli Studi di Milano) and Juan Caballero (IMDEA Software Institute).

4. Arianna Blasi. *Using Semantic Similarity Analysis of Javadoc Comments to Automatically Generate Test Oracles*. Master Thesis. Università degli Studi di Milano-Bicocca. October 2017. Advisors: Mauro Pezzé (Università degli Studi di Milano-Bicocca), Alessandra Gorla (IMDEA Software Institute).

5. Sergio Delgado Castellanos. *ToraDocu – Generación Automática de Casos de Test con Oráculos*. Master Thesis. Universidad Politécnica de Madrid. June 2017. Advisors: Damiano Zanardini (UPM), Alessandra Gorla (IMDEA Software Institute).

6. Bogdan Kulynych. *ClaimChain: Decentralized Public key Infrastructure*. Master Thesis. Universidad Politécnica de Madrid. July 2017. Advisor: Manuel Carro and Carmela Troncoso (IMDEA Software Institute).

7. Chiara Redaelli. *On Fully Homomorphic Encryption from the Learning with Errors Problem*. Master Thesis. Università degli Studi di Milano-Bicocca, March 2017. Advisors: Francesca Dalla Volta (Università degli Studi di Milano-Bicocca), Dario Fiore (IMDEA Software Institute), Luca Nizzardo (IMDEA Software Institute).

8. María del Carmen Sánchez Medrano. *Enhancing Online Banking Authentication Using Keystroke Dynamics*. Master Thesis. Máster Universitario en Software y Sistemas (MUSS), Escuela Técnica Superior de Ingenieros Informáticos, Universidad Politécnica de Madrid. July 2017. Advisor: Juan Caballero (IMDEA Software Institute).

9. Sergio Valverde García. *Automatic Testing Platform for Android Apps*. Master Thesis. Universidad Politécnica de Madrid. June 2017. Advisors: Antonio LaTorre (UPM), Alessandra Gorla (IMDEA Software Institute).

10. Inés Blázquez Ballesteros. *Implementation of a Random Search Rule in Logic Programming*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). June 2017. Advisor: Manuel Hermenegildo and José Francisco Morales.

11. Sergio Chica Manjarrez. *Diseño e Implementación de un Módulo para Identificar Código Compartido entre Ejecutables Maliciosos*. Bachelor Thesis. Grado en Ingeniería Informática. Escuela Técnica Superior de Ingenieros Informáticos, Universidad Politécnica de Madrid. June 2017. Advisor: Juan Caballero (IMDEA Software Institute).

12. Anais Querol Cruz. *Cryptographic Methods for Secure Delegation of Computation in Electronic Voting Applications*. Bachelor Thesis. Universidad Politécnica de Madrid. June 2017. Advisors: Manuel Carro, Dario Fiore (IMDEA Software Institute).

13. Silvia Sebastián González. *Diseño e Implementación de un Módulo para la Detección de Aplicaciones Móviles Maliciosas en Mercados Online*. Bachelor Thesis. Grado en Ingeniería Informática. Escuela Técnica Superior de Ingenieros Informáticos, Universidad Politécnica de Madrid. June 2017. Advisor: Juan Caballero (IMDEA Software Institute).

Invited talks

6.2 Invited Talks

6.2.1 Invited and Plenary Talks by IMDEA Scientists

1. *Miguel Ambrona*. Criptografía, seguridad probable. Invited talk at Universidad Complutense de Madrid, Red de Doctorandos en Matemáticas. UCM, Madrid, March 23rd, 2017.

2. *Gilles Barthe*. Advances in Computer-Aided Cryptography. Invited talk at EUROCRYPT 2017. Paris, France. May 2017.

3. *Gilles Barthe*. Relational Verification of Higher-Order Probabilistic Programs. APLAS 2017. Suzhou, China. November 2017.

4. *Juan Caballero*. The Rise of Potentially Unwanted Programs: Measuring its Prevalence, Distribution, and Economics. Keynote at 7th Software Security, Protection and Reverse Engineering Workshop (SSPREW). Orlando, FL, USA. December 2017.

5. *Juan Caballero*. The Rise of Potentially Unwanted Programs: Measuring its Prevalence, Distribution, and Economics. Invited talk at Cybersecurity With The Best. October 2017.

6. *Juan Caballero*. The Rise of Potentially Unwanted Programs: Measuring its Prevalence, Distribution, and Economics. Invited talk at 40th Annual meeting of the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG). Lisbon, Portugal. June 2017.

7. *Dario Fiore*. Computing Quadratic Functions on Encrypted Data. Invited talk at Mathcrypt 2017. Daejeon, South Korea. June 2017.

8. *Dario Fiore*. Homomorphic Authentication for Computing Securely on Untrusted Machines. Keynote at the 22nd Nordic Conference on Secure IT Systems (NordSec 2017), Tartu, Estonia. November 2017.

9. *Isabel García*. Code Search: A Semantic, Abstract-Interpretation Based Approach. Talk as recipient of the SISTEDES/Accenture Technology Best Master Thesis prize in Software Development Tools and Methodologies, at Jornadas SISTEDES. La Laguna, Tenerife. July 2017.

10. *Roberto Giacobazzi*. Securing Code — Hacking the precision of program analysis. Fall Days on System and Software Analysis. Nunspeet, the Netherlands, November 6-10, 2017.

11. *Alessandra Gorla*. Inferring Procedure Specifications for Automated Testing. Invited speaker at the CHOOSE forum 2017 on Software and Data Engineering. Zurich, Switzerland. 17 November 2017.

12. *Alessandra Gorla*. Mining the Google Play for Anomalies. Keynote speaker at the 2017 WAMA workshop. Paderborn, Germany. September 2017.

13. *Alexey Gotsman*. Towards Modular Verification of Consensus Protocols. RainbowFS Workshop on Consistency in Distributed Storage Systems, Université Pierre et Marie Curie–LIP6. Paris, France. May 2017.

14. *Manuel Hermenegildo*. From Logic Programming to Constraint Programming. Plenary invited talk at the special session in memory of Alain Colmeraruer in the joint 20th International Conference on Theory and Applications of Satisfiability Testing, 23rd International Conference on Principles and Practice of Constraint Programming, and 33rd International Conference on Logic Programming. Melbourne, Australia. August 2017.

15. *Manuel Hermenegildo*. Energy Consumption Analysis and Verification. Invited talk at the Fifth International Workshop on Verification and Program Transformation, VPT 2017. Uppsala, Sweden. April 2017.

16. *Boris Köpf*. Static Quantification of Timing Side Channels. Invited speaker at "Workshop on Formal Methods and Tools for Security" (FMATS5). Cambridge, UK. September 2017.

17. *Boris Köpf*. Static Analysis of Timing Side Channels. Invited speaker at "IACR Spring School on Security & Correctness in the Internet of Things". Graz, Austria. May 2017.

18. *Boris Köpf*. Formal Methods for Reliable Software Security. Invited panelist at the Final Event of the DFG Project "Reliably Secure Software Systems". Darmstadt, Germany. September 2017.

19. *Pedro López-García and Manuel Hermenegildo*. User-Definable Resource Bounds Analysis for Logic Programs. Plenary invited talk at the 33rd International Conference on Logic Programming. Melbourne, Australia. August 2017.

20. *Pedro López-García*. Static Profiling of Parametric Resource Usage as a Valuable Aid for Hot-spot Detection. Invited talk at the 15th International Colloquium on Implementation of Constraint and LOgic Programming Systems (CICLOPS'17). Melbourne, Australia. August 2017.

21. *Carmela Troncoso*. Systematic Privacy by Design engineering. Talk at ISSS EU-Datenschutzgrundverordnung und nues CH-DSG. Zurich, Switzerland. June 2017.

22. *Carmela Troncoso*. Privacy-Preserving Systems: Systematic Reasoning for Design and Evaluation. Talk at 2nd INTERPOL Workshop on Privacy Enhancing Technologies. Lyon, France. January 2017.

23. *Pepe Vila*. Loophole: Timing Attacks on Shared Event Loops in Chrome. RootedCON. Madrid, Spain. March 2017.

24. *Pepe Vila*. Loophole: Timing Attacks on Shared Event Loops in Chrome. CRYPTACUS 2017. Nijmegen, Netherlands. November 2017.

6.2.2 Invited Seminars and Lectures by IMDEA Scientists

1. *Miguel Ambrona*. Workshop on Cryptography and Internet Security. Semana de la Ciencia Complutense (Co-organizer). Madrid, Spain. November 2017.

2. *Miguel Ambrona*. Generic Transformation of Predicate Encodings: Constructions and Applications. NTT Laboratories. Tokyo, Japan. May 2017.

3. *Joaquín Arias*. Description and Evaluation of Modular TCLP. Doctoral Consortium (Universidad Politécnica de Madrid). Madrid, Spain. March 2017.

4. *Joaquín Arias*. Description and Evaluation of a Generic Design to Integrate CLP and Tabled Execution. University of Texas at Dallas. Dallas, USA. July 2017.

5. *Juan Caballero*. The Rise of Potentially Unwanted Programs: Measuring its Prevalence, Distribution, and Economics. Invited talk at Universidade da Lisboa. Lisbon, Portugal. June 12th, 2017.

6. *Paolo Calciati*. How do Apps Evolve in Their Permission Requests? A preliminary Study. 10th Seminar on Advanced Techniques & Tools for Software Evolution (SATToSE 2017). Madrid, Spain. June 2017.

7. *Ignacio Fábregas*. When Are Prime Formulae Characteristic? Cosynus Seminar Series Institution: Laboratoire d'informatique de l'École Polytechnique (LIX). Palaiseau, France. March 2017.

8. *Dario Fiore*. On the (In)Security of SNARKs in the Presence of Oracles. II CryptoAction Symposium, Amsterdam, The Netherlands. March 2017.

9. *Álvaro García*. Towards Modular Verification of Consensus Protocols. The Aarhus Concurrency Workshop (ACW 2017). Aarhus, Denmark. May 2017.

10. *Álvaro García*. Rule Formats for Nominal Process Calculi. 28th International Conference on Concurrency Theory (CONCUR 2017). Berlin, Germany. September 2017.

11. *Miriam García*. A CEGAR Approach for Stability Verification of Linear Hybrid System. Second Workshop on Design and Analysis of Robust Systems (DARS). Heidelberg, Germany. July 2017.

12. *Miriam García*. An Algorithmic Approach for Stability Verification of Hybrid System. Tesis (Doctoral), E.T.S. de Ingenieros Informáticos. UPM, Madrid, Spain. July 2017.

13. *Alessandra Gorla*. Software Testing and its Automation. Guest lecture at CERN summer school, UPM, Madrid. September 2017.

14. *Manuel Hermenegildo and Pedro López*. Cost Analysis with Recurrence Relations (using CiaoPP). Invited tutorial at Dagstuhl Seminar on Resource Bound Analysis. Schloss Dagstuhl, Germany. July 2017.

15. *Manuel Hermenegildo and Pedro López*. Energy Consumption Analysis and Verification. Invited lecture at Dagstuhl Seminar on Resource Bound Analysis. Schloss Dagstuhl Germany. July 2017.

16. *Boris Köpf*. Static Quantification of Timing Side Channels. ARM Cambridge. Cambridge, UK. July 2017.

17. *Boris Köpf*. Static Quantification of Timing Side Channels. KTH Stockholm. Stockholm, Sweden. October 2017.

18. *Platon Kotzias*. An analysis of Pay-Per-Install Economics Using Entity Graphs. International Computer Science Institute, University of Berkeley. Berkeley, USA. June 2017.

19. *Platon Kotzias*. Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services. JNIC 2017. Madrid, Spain. September 2017.

20. *Srdjan Matic*. Dissecting Tor Bridges: a Security Evaluation of Their Private and Public Infrastructures. JNIC 2017. Madrid, Spain. September 2017.

21. *Srdjan Matic*. Dissecting Tor Bridges: a Security Evaluation of Their Private and Public Infrastructures. Saarland University. Saarbrücken, Germany. October 2017.

22. *Luca Nizzardo*. Cryptography: Past, Present and Future Challenges. IBM-Intesa Sanpaolo joint meeting at Intesa Sanpaolo, The New York Branch. New York, USA. February 2017.

23. *Luca Nizzardo*. Multi-Key Homomorphic Authenticators. CAISS Reading Group at City College of New York. New York, USA. March 2017.

24. *Luca Nizzardo*. Multi-key Homomorphic Authenticators. Cornell Tech Spring Reading Group. Cornell Tech, New York, USA. April 2017.

25. *Luca Nizzardo*. Multi-Key Homomorphic Authenticators. JNIC 2017. Madrid, Spain. September 2017.

26. *Luca Nizzardo*. Cryptography & Business: State of the Art and Future (?) Challenges. IBM Italia SpA. Segrate, Milano, Italy. September 2017.

27. *Richard Rivera*. AVCLASS: A Tool for Massive Malware Labeling. JNIC 2017. Madrid, Spain. June 2017.

28. *Carmela Troncoso*. Privacy by design. Summer school on Real-World Crypto and Privacy, Sibenik, Croatia, June 2017.

29. *Carmela Troncoso*. Introduction to Traffic Analysis. Summer school on real-world crypto and privacy, Sibenik, Croatia, June 2017.

30. *Carmela Troncoso*. Dissecting Tor Bridges: a Security Evaluation of their Private and Public Infrastructures. School of Computer Science and Statistics at Trinity College. Dublin, Ireland, March 2017.

31. *Guillermo Vigueras*. Machine Learning-Driven Transformations for C Programs. Departamento de Informática, Universidad Carlos III de Madrid. Madrid, Spain. February 2017.

32. *Pepe Vila*. RFID Security. Lecture at the Computer Security Class of UPM's Master Universitario en Software y Sistemas. Madrid, Spain. December 2017.

6.2.3 Invited Speaker Series

During 2017, 28 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. *Miguel Á. Carreira-Perpiñán*. Professor, University of California at Merced, USA: Learning Binary Hash Functions for Information Retrieval Applications.

2. *Goran Doychev*. Researcher, Independent Researcher: Rigorous Analysis of Software Countermeasures against Cache Attacks.

3. *Hongseok Yang*. Professor, University of Oxford, UK: Probabilistic Programming.

4. *Rupak Majumdar*. Scientific Director, Max Planck Institute for Software Systems: Hitting Families of Schedules.

5. *Alfredo Pironti*. Researcher, IOActive: 15 Years of Broken Encrypted Emails... and We're Still Doing It Wrong.

6. *Ignacio Fabregas*. Post-doctoral Researcher, Universidad Complutense de Madrid, Spain: Logics for Process Semantics.

7. *Daniel Riofrio*. Post-doctoral Researcher, University of New Mexico, USA: The Presidential Elections in Ecuador during the digital era.

8. *Alberto López*. General Secretary, Escuela Universitaria de Diseño, Innovación y Tecnología: Software research activities in Design at ESNE.

9. *Sebastian Mödersheim*. Associate Professor, Technical University of Denmark: Alpha-Beta-Privacy – Defining Privacy is Supposed to be Easy.

10. *Andreas Rossberg.* Software Engineer, Google: Bringing the Web up to Speed with WebAssembly.

11. *Rebekah Overdorf.* Ph.D. Student, Drexel University, USA: How Unique is Your .onion? An Analysis of the Fingerprintability of Tor Onion Services.

12. *Azalea Raad.* Ph.D. Student, Imperial College, London: Local Reasoning for Concurrency, Distribution and Web Programming.

13. *Romain Gay.* Ph.D. Student, ENS Paris: Improved Dual System ABE in Prime-Order Groups via Predicate Encodings.

14. *Ilya Sergey.* Lecturer, University College London, United Kingdom: Programming and Proving with Distributed Protocols.

15. *Daniel Benarroch.* Lead Cryptographer, QED-it, Israel: Computing on Private Data with Zero-Knowledge Proofs and the Blockchain.

16. *Julian Dolby.* Research Staff Member, IBM T. J. Watson Research Center, USA: WALA Everywhere.

17. *Grigory Fedyukovich.* Post-doctoral Researcher, University of Washington, USA: Synchronizing Constraint Horn Clauses.

18. *Christian Hammer.* Full Professor, University of Potsdam, Germany: WebPol: Fine-grained Information Flow Policies for Web Browsers.

19. *Ana Sokolova.* Associate Professor, University of Salzburg, Austria: Concurrent Data Structures: Semantics and Relaxations.

20. *William Suski.* Science Director, Office of Naval Research Global, USA: ONR Global Basic Research Funding Opportunities.

21. *Monir Azraoui.* Post-doctoral Researcher, EURECOM, France: Secure Operations in the Cloud.

22. *Filippo Bonchi.* Research Scientist, École normale supérieure (ENS), Lyon, France: Full Abstraction for Signal Flow Graphs.

23. *Gregory Chockler.* Professor, Royal Holloway, University of London (RHUL): The Space Complexity of Reliable Storage Services.

24. *Veelasha Moonsamy.* Post-doctoral Researcher, Radboud University, The Netherlands: Side-channel Attacks on Mobile Devices and Future Research Directions.

25. *Danil Annenkov.* Ph.D. Student, DIKU University of Copenhagen, Denmark: Reasoning Techniques for the Module System Formalisation in Coq.

26. *Vasilios Mavroudis.* Ph.D. Student, University College London, United Kingdom: Cryptographic Hardware from Untrusted Components.

27. *Borzoo Bonakdarpour.* Assistant Research Professor, McMaster University, Canada: Automated Fine-Tuning of Probabilistic Self-Stabilizing Algorithms.

28. *Giulia De Santis.* Ph.D. Student, INRIA Nancy-Grand Est., France: Classifying Internet-wide scanners using Gaussian Mixture and Hidden Markov Models.

6.2.4 Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of **26** seminars were given in 2017.

6.3 Scientific Service and Other Activities

6.3.1 Conference and Program Committee Chairmanship

Juan Caballero:

1. TPC co-chair for ACSAC 2017, the 2017 Annual Computer Security Applications Conference.

Alessandra Gorla:

2. Artifact Evaluation co-chair, International Conference on Software Maintenance and Evolution (ICSME 2017).

Alexey Gotsman:

3. PC Co-chair of the Workshop on Principles and Practice of Consistency for Distributed Data (PAPOC 2017).

Manuel Hermenegildo:

4. Co-chair of the 4th Workshop on Horn Clauses for Verification and Synthesis (HCVS 2017). Sweden.

Boris Köpf:

5. PC Co-chair of the 29th IEEE Computer Security Foundations Symposium (CSF 2017).

José Francisco Morales:

6. PC co-chair of the 15th International Colloquium on Implementation of Constraint and LOgic Programming Systems (CICLOPS 2017).

Aleks Nanevski:

7. PC co-chair of 6th ACM SIGPLAN Workshop on Higher-order Programming with Effects (HOPE 2017).

Nataliia Stulova:

8. PC co-chair of the 15th International Colloquium on Implementation of Constraint and LOgic Programming Systems (CICLOPS 2017).

Carmela Troncoso:

9. Caspar Bowden PET Award Chair (2017).

10. General Chair IEEE International Workshop on Information Forensics and Security (2017).

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. Advisory board of the Information Security and Cryptography series.

4. Steering committee of EATCS/ETAPS/SIGLOG/SIGPLAN Summer School.

5. Steering committee of EuroS&P—European Symposium on Security and Privacy.

6. Steering committee of ETAPS—European Joint Conferences on Theory and Practice of Software.

7. Steering committee of International School on Foundations of Security Analysis.

Juan Caballero:

8. Editorial Board of the ACM Transactions in Privacy and Security (ACM TOPS).

9. Steering committee of Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).

10. Steering committee of Jornadas Nacionales de Investigación en Ciberseguridad (JNIC).

11. Steering Committee of the International Symposium on Engineering Secure Software and Systems (ESSoS).

Dario Fiore:

12. Editorial Board of IET Information Security Journal

13. Editor Board of the International Journal of Applied Cryptography.

Manuel Hermenegildo:

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

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

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

17. Steering Committee of the Conference on Compiler Construction (CC).

18. Editorial Advisor and former Area Editor (architecture and implementation) of “Theory and Practice of Logic Programming” (Cambridge U. Press).

19. Associate Editor of the “Journal of New Generation Computing” (Springer-Verlag).

20. Area Editor of “Journal of Applied Logic” (Elsevier North-Holland).

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

Boris Köpf:

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

23. Steering committee of ETAPS Conference on Principles of Security and Trust (POST).

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

Pedro López:

25. Steering Committee of the International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR).

Carmela Troncoso:

26. Editorial Board of Proceedings of Privacy Enhancing Technologies.

27. Member of Privacy Enhancing Technologies Symposium Board (PETS Steering Committee).

6.3.3 Participation in Program Committees

Gilles Barthe:

1. 38th IEEE Symposium on Security and Privacy (S&P 2017).

2. 2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017).

3. 23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2017).

4. 33rd Conference on the Mathematical Foundations of Programming Semantics (MFPS 2017).

5. 37th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2017).

Manuel Carro:

6. 33rd International Conference on Logic Programming (ICLP 2017).

7. 15th International Conference on Service Oriented Computing (ICSOC 2017).

8. 19th International Symposium on Practical Aspects of Declarative Languages (PADL 2017).

9. XVII Jornadas sobre Programación y Lenguajes (PROLE 2017).

Dario Fiore:

10. 5th Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC 2017).

11. 21st International Conference on Financial Cryptography and Data Security 2017 (FC 2017)

12. 20th International Conference on Practice and Theory of Public-Key Cryptography (PKC 2017).

13. 2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017).

14. 9th ACM Cloud Computing Security Workshop (CCSW 2017).

15. 23rd Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2017).

Pierre Ganty:

16. 4th Workshop on Horn Clauses for Verification and Synthesis (HCVS 2017).

17. 24th International Static Analysis Symposium (SAS 2017).

18. 4th International Conference on Tools and Methods of Program Analysis (TMPA 2017).

Álvaro García:

19. Combined 24th International Workshop on Expressiveness in Concurrency and 14th Workshop on Structural Operational Semantics (EXPRESS/SOS 2017).

Alessandra Gorla:

20. IEEE and ACM International Conference on Automated Software Engineering (ASE 2017).

Alexey Gotsman:

21. 26th European Symposium on Programming (ESOP 2017).

22. Workshop on Programming Models and Languages for Distributed Computing (PMLDC 2017).

23. 12th ACM SIGPLAN Workshop on Transactional Computing (TRANSACT 2017).

Manuel Hermenegildo:

24. 33rd International Conference on Logic Programming (ICLP 2017).

Boris Köpf:

25. ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS 2017).

26. 14th International Conference on Quantitative Evaluation of Systems (QEST 2017).

27. 4th International Conference on Tools and Methods of Program Analysis (TMPA 2017).

28. 6th ETAPS Conference on Principles of Security and Trust (POST 2017).

29. 5th Workshop on Hot Issues in Security Principles and Trust (HotSpot 2017).

Pedro López:

30. 4th Workshop on Horn Clauses for Verification and Synthesis (HCVS 2017).

José Francisco Morales:

31. 27th International Symposium On Logic-Based Program Synthesis And Transformation (LOPSTR 2017).

Richard Rivera:

32. 3rd International Conference on Technology Trends (CITT 2017).

César Sánchez:

33. 2nd International Workshop in PrePost (Pre- and Post-Deployment Verification Techniques).

34. 7th IPM International Conference on Fundamentals of Software Engineering (FSEN 2017).

35. 17th International Conf. on Runtime Verification (RV 2017).

36. XVII Jornadas sobre Programacion y Lenguajes (PROLE 2017).

Carmela Troncoso:

37. 38th IEEE Security and Privacy Symposium (IEEE S&P 2017).

38. 24th ACM Conference on Computers and Communications Security (ACM CCS 2017).

39. 11th ACM Asia Conference on Computers and Communications Security (ACM ASIA CCS 2017).

6.3.4 Association and Organization Committees

Gilles Barthe:

1. Co-organizer or *ProbProgSchool 2017*, a summer school on probabilistic programming in Braga, Portugal.

Dario Fiore:

2. Vice-Chair and Management Committee member (representing Spain) of COST Action IC1306 “Cryptography for Secure Digital Interaction”.

Manuel Hermenegildo:

3. President of the INRIA Scientific Council (Institut National de Recherche en Informatique et en Automatique, France).

4. Vice-President of Informatics Europe. Elected member of the executive board. Member of the department evaluation board. Member of the Strategy Special Group. Member of the Research Evaluation Group.

5. Member *Academia Europaea*.

6. Member of Schloss Dagstuhl Scientific Advisory Board (Germany).

7. Director, EIT Digital Madrid Node.

8. Chair, EIT Digital Madrid Node Steering Committee.

9. Steering Board member, EIT Digital.

10. Member of the IRILL Scientific Advisory Board (French Institute for Free Software).

11. Member of the External Advisory Board of the NOVA LINCS Institute (Portugal).

12. Secretary of the International Association for Logic Programming.

13. Member of the International Federation for Computational Logic (IFCoLog) Advisory Board.

14. Member of the Technical University of Madrid Consulting Council.

15. Member of the Technical University of Madrid Gallery of Distinguished Members.

Carmela Troncoso:

16. Co-organizer of the *Summer School on Real-World Crypto and Privacy* in Sibenik, Croatia.

6.4 Awards

Paper Awards:

1. Jorge Navas, Edison Mera, *Pedro López-García*, and *Manuel Hermenegildo*. User-Definable Resource Bounds Analysis for Logic Programs. 33rd International Conference on Logic Programming (ICLP 2017). **10 year Test of Time Award**.

2. Antonio Nappa, M. Zubair Rafique, *Juan Caballero*. Driving in the Cloud: An Analysis of Drive-by Download Operations and Abuse Reporting. DIMVA 2017, paper published at DIMVA 2013. **Most Influential DIMVA Paper 2009-2013**.

3. *Pablo Cañones*, *Boris Köpf*, and Jan Reineke. Security Analysis of Cache Replacement Polices. Proceedings 6th Conference on Principles of Security and Trust (POST '17). **Nominated for the EATCS award for the best ETAPS paper in theoretical computer science**.

4. *P. Vila* and *B. Köpf*. Loophole: Timing Attacks on Shared Event Loops in Chrome. USENIX Security 2017. **Distinguished Paper Award**.

5. *Carolina Dania* and Marina Egea. SQL-PL4OCL: An automatic Code Generator from OCL to SQL Procedural Language. MoDELS 2017, Austin, Texas, USA. **Journal of Software and Systems Modeling Best Paper Award**.

6. *P. Calciati* and *A. Gorla*. How do Apps Evolve in Their Permission Requests? A preliminary Study. 10th Seminar on Advanced Techniques & Tools for Software Evolution (SATToSE 2017). **Distinguished Paper Award**.

Thesis Awards:

7. *G. Doychev*. Tools for the Evaluation and Choice of Countermeasures against Side-Channel Attacks. Universidad Politécnica de Madrid, 2016 (awarded in 2017). **UPM Outstanding Ph.D. Thesis Award**.

8. *I. García*. Code Search: A Semantic, Abstract-Interpretation Based Approach. Universidad Politécnica de Madrid, 2017. **SISTEDES/Accenture Technology Best Master Thesis prize in Software Development Tools and Methodologies**.

Other Awards:

9. *C. Troncoso*. IEEE Security and Privacy Symposium 2017. **Best Reviewer Award**.

10. *C. Troncoso*. Engineering Privacy by Design Reloaded. **CNIL-INRIA Privacy Award 2017**.

11. *B. Kulynych*. **Diploma at ActuaUPM** entrepeneurship competition, for his project "Private Common Data Analytics".

awards

education

6.5 Education

While the Institute focuses on research and technology transfer, our researchers are sometimes involved in teaching courses offered by universities and other entities. The following is a list of courses where IMDEA Software researchers taught in 2017.

1. Software Construction: Implementation Issues (Master level, 6 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Alexey Gotsman*, *Carmela Troncoso*

2. Independent Study with Adviser (Master level, 6 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *César Sanchez*, *Carmela Troncoso*.

3. Directed Study with Adviser (Master level, 6 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *César Sánchez*.

4. Software Construction: Analysis of Requirements (Master level, 6 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Juan Caballero*,*César Sánchez*.

5. Software Construction: Architecture and Interface Design (Master level, 6 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Juan Caballero*, *Alexey Gotsman*, *César Sanchez*.

6. Computer Security (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Juan Caballero*, *Dario Fiore*, *Alessandra Gorla*, *Boris Koepf*.

7. Advanced Computer Security (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Juan Caballero*, *Dario Fiore*, *Alessandra Gorla*, *Boris Koepf*.

8. Formal Methods for Concurrent and Reactive System (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Alexey Gotsman*, *César Sánchez*.

9. Abstract Interpretation (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Pierre Ganty*.

10. Rigorous Software Development (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Manuel Carro*, Julio Mariño.

11. Data Structures and Algorithms (Undergraduate level, 6 ECTS). Grado en Ingeniería Informática, Universidad Politécnica de Madrid (UPM). *Manuel Carro*.

12. Declarative Programming: Logic and Constraints (Undergraduate level, 3 ECTS). Grado en Ingeniería Informática, Universidad Politécnica de Madrid (UPM). Francisco Bueno, *Manuel Hermenegildo*, Miguel García, M. Carmen Suárez.

13. Logic and Constraint Programming. Universidad Politécnica de Madrid (UPM).

6.6 Dissemination Events

In 2017 IMDEA Software researchers have participated in multiple events related to dissemination and the promotion of science.

Researcher's Night.

In September 2017, as in previous years, the IMDEA Software Institute participated in the European-wide initiative "Researchers' Night". This year's event was titled "IMDEA-CSI: Crime Scene Investigation". In collaboration with the other IMDEA Institutes and with the support of the Spanish National Police, the event focused on how science and technology can help in solving a crime, finding the criminal and its motivation. The event represented the crime scene of a robbery, with a fatal victim, being investigated by three real agents from the Spanish National Police. During the investigation, researchers from the IMDEA Institutes presented how research helps the different steps of a police investigation from evidence collection to data analysis and determining the criminal's identity.

The IMDEA Software Institute was represented in the event by researchers Manuel Carro (Director) and Juan Caballero (Deputy Director). The event took place at the Residencia de Estudiantes on Friday, September 29th and was a real success, attracting a great affluence of public that filled the auditorium.

This year's event achieved a significant amount of dissemination on national and regional media, in part due to the involvement of the Spanish National Police.

The following interviews on radio and television helped to spread the word about the event:

• Manuel Carro, the Institute's director, was interviewed about science and the European Researchers' Night by the National TV program La Tarde en 24 Horas. The 20-minute interview was performed by journalist Carmen Romero Marí and aired on September 21st.

• On September 14th, the IMDEA Institutes participated in the live radio show Primera Hora, hosted by Javier García Mateo in Gestiona Radio. During one hour, they spoke about science in general and, in particular, about their European Researchers' Night activity. The IMDEA Software Institute was represented in the radio show by researchers Manuel Carro (Director) and Juan Caballero (Deputy Director).

• Manuel Carro (Director) was interviewed live in the "La Tarde" program of COPE, one of the main Spanish radio stations. The interview was performed by journalist Ángel Expósito on Sep. 29th.

"Con ciencia en la escuela".

In March 2017, the IMDEA Software Institute, together with the IMDEA Nanoscience Institute, took part in the yearly event "Con ciencia en la escuela" (a play on words — the literal meaning is "With Science in the School", but it its pronunciation is the same as "Awareness in the School"). This is an educational event aimed at bringing science closer to the public, addressing specially children in primary and secondary education. In the same event, other research institutions and schools presented interactive and enticing experiments with the goal of fostering STEM (and related) vocations. The Institute presented three demos in which attendees learned about cryptography, side channel attacks on Web browsers, and automated testing.

The event was organized by Círculo de Bellas Artes and FUHEM, with the collaboration of the Foundation madri+d, the publisher *Editorial SM*, The *Cooperativa de Enseñanza José Ramón Otero*, the Madrid Regional Ministry for Education, Youth and Sports (later in the year renamed to Education and Innovation), and the Spanish Foundation for Science and Technology (FECYT) .

Computer Science Podcasts.

Juan José Moreno, Research Professor, and Manuel Carro, Director, were the main speakers in two installments of the podcast "1 bit of memory", part of a series of episodes focusing on the lives and achievements of the Turing Award recipients. This series of podcasts aimed at explaining easily the Turing awardees' work and how it has influenced Computer Science and society at large.

Ten Years of ERC.

In 2017, the European Research Council (ERC) celebrated its 10th anniversary. IMDEA Software ERC grantholders Aleks Nanevski and Alexey Gotsman, together with the Institute's director Manuel Carro, attended the 10-year celebration that took place at the Royal Botanic Garden in Madrid on June 12. Besides informative and celebratory talks, several ERC awardees from the Madrid Region presented their experience and their research.

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 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 2017 included the following:

1. EIT Digital: Opening of EIT Digital as full node. March 2017.

2. EIT Digital/UPM: Entrepreneurship course on Opportunity Recognition. June 2017.

3. EIT Digital/UPM: Data Science Master Welcome Day. September 2017.

4. EIT Digital: Cybersecurity Matchmaking event. November 2017.

5. EIT Digital: Innovation Day and Digital Wellbeing Challenge Finals. November 2017.

scientific highlights

annual report 2017

a rigorous approach to consistency in cloud databases

A Rigorous Approach to Consistency in Cloud Databases

The past decade has witnessed a spectacular growth of cloud-based Internet services. Web sites such as Amazon and Facebook process hundreds of thousands of user requests per second, yet stay available at all times. To achieve this, the shared data accessed by the requests is managed by novel *cloud databases*, which partition and replicate the data across a large number of nodes and/or a wide geographical span. To achieve high availability and scalability, cloud databases need to maximize the parallelism of data processing. Unfortunately, this leads them to weaken the guarantees they provide about data consistency to applications. The resulting programming models are very challenging to use correctly, and we currently do not have advanced methods and tools that would help programmers in this task.

The goal of the project is to develop a synergy of novel reasoning methods, static analysis tools and database implementation techniques that maximally exploit parallelism inside cloud databases, while enabling application programmers to ensure correctness. We intend to achieve this by first developing methods for reasoning formally about how weakening the consistency guarantees provided by cloud databases affects application correctness and the parallelism allowed inside the databases. This will build on techniques from the areas of programming languages and software verification. Our theory will then serve as a basis for practical implementation techniques and tools that harness database parallelism, but only to the extent such that the side effects of the parallelism do not compromise application correctness. This is a rigorous approach to the problem of data consistency in cloud databases that aims to push the envelope in their availability, scalability and cost-effectiveness.

The mathematical models and reasoning methods developed in the project will enable programming language and verification researchers to further improve the quality of applications using cloud databases. By applying the theory of cloud databases to their implementations, the project will also allow systems researchers to design these databases in a more principled way, informed by the consistency requirements of applications using them. Finally, the project will address a pressing need of the software industry

Unión Europea

erc

for systematic techniques to scalably manage data consistency. The rigorous approach promoted by the project can facilitate constructing large-scale services that are correct, yet maximally exploit the parallelism enabled by cloud computing. Increased parallelism will allow achieving better availability and scalability with fewer resources, thus lowering costs and helping the industry cope with ever growing pressures on its infrastructure. In the end, these technological advances will benefit the society as a whole, by enabling more reliable and affordable Internet services that all of us use every day.

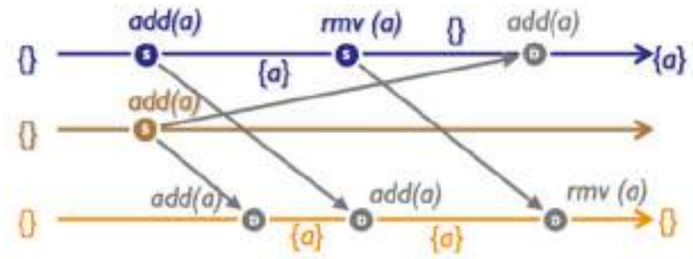
The research in the above project is supported by an ERC Starting Grant RACCOON held by Alexey Gotsman during 2017-2021.

Related publications

[1] *Alexey Gotsman*, Hongseok Yang, Carla Ferreira, Mahsa Najafzadeh, and Marc Shapiro. 'Cause I'm strong enough: reasoning about consistency choices in distributed systems. POPL'16: Symposium on Principles of Programming Languages, St. Petersburg, FL, USA, pages 371-384. ACM, 2016.

[2] *Andrea Cerone* and *Alexey Gotsman*. Analysing snapshot isolation. PODC'16: Symposium on Principles of Distributed Computing, Chicago, IL, USA, pages 55-64. ACM, 2016.

cassandra amazon DynamoDB Microsoft Azure DocumentDB riak



type and proof structures for concurrent software verification

Type and Proof Structures for Concurrent Software Verification

Chip manufacturers today have reached, due to thermal limits and other considerations, processing speed ceilings for computer processors. This leaves concurrent programming, where one program executes on many processors, as the only way to scale our computing power.

Unfortunately, concurrent programs are notoriously difficult to write because of the complexity of interaction between their components. This complexity comes into the sharpest focus if one tries to develop a mathematical, computer-checkable proof that a concurrent program produces the desired result. The required effort for developing such a proof today is overwhelming even for the simplest concurrent programs, because of the combinatorial explosion associated with the component interaction.

The goal of the Mathador project is to study, decompose, and simplify the structure of mathematical proofs of concurrent programs, to the point where they can be developed on a regular basis. Mastering these proofs will mean that we know how to describe the interaction between concurrent components in an intellectually manageable way. In turn, this will directly impact how we think about, write, and understand concurrent software.

The starting point in this task is the well-known idea in theoretical computer science that programs and mathematical proofs share common foundations in constructive mathematics. One can thus apply programming ideas, such as abstraction and information hiding, to control the combinatorial explosion that is inherent in proofs. The project's goal is then to develop constructive mathematical theories that will facilitate engineering of practically feasible computer-checkable proofs for concurrent programs.

The Mathador project is supported by an ERC Consolidator Grant awarded to Aleks Nanevski for 2017-2021.

Unión Europea

Related publications

[1] Aleksandar Nanevski. *Separation Logic and Concurrency.* Lecture notes for Oregon Programming Languages Summer School (OPLSS'16), June 2016. https://software.imdea.org/~aleks/oplss16/notes.pdf

[2] Ruy Ley-Wild and Aleksandar Nanevski. *Subjective auxiliary state for coarse-grained concurrency.* Proceedings of the 40th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL'13), pages 561–574, ACM Press, 2013.

[3] Ilya Sergey, Aleksandar Nanevski and Anindya Banerjee. *Mechanized Verification of Fine-grained Concurrent Programs.* Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'15), pages 77-87, ACM Press, 2015.

online banking

monitoring

Online Banking Anti-Fraud Monitoring

The most common approach in online banking for authenticating users is through credentials, i.e., a user identifier and a password. Unfortunately, this is a method of easy impersonation because credentials may be guessed or stolen. While most banks limit brute force guessing attacks by blocking the account after a maximum number of failed login attempts, this defense does not help when the user credentials are stolen, e.g., through a phishing attack.

A critical challenge for banks is to determine whether the user undergoing online banking authentication is the real owner of the account, rather than an attacker that stole the account owner's credentials. Security defenses based on biometrics have proven very powerful against such impersonation attacks. However, most biometrics defenses have two drawbacks: they are expensive to implement and their usability is low since they require special hardware. Fortunately, there exist a class of biometric defenses based on

Anti-Fraud

keystroke dynamics that overcome these drawbacks. Keystroke dynamics defenses are based on each user having a distinct typing pattern, which includes the timing between keys being typed and the control characters used. Such features uniquely identify a user, are unknown to the attacker, are difficult to replicate, and their usability is high since they are transparent to the user.

In this project we are building a commercial service against user account impersonation for online banking. Our solution builds on novel approaches for user profiling through machine learning algorithms based on keystroke dynamics features. The project is funded by EIT Digital during 2017. It involves a consortium of three European partners: the IMDEA Software Institute, in charge of the keystroke dynamics data collection and feature extraction; Security Reply, an Italian security company that acts as business champion and will offer the commercial service in its portfolio; and Fondazione Bruno Kessler, an Italian research institute in charge of the machine learning component.

loophole: timing

Loophole: Timing Attacks on Shared Event Loops in Chrome

Event-driven programs define responses to events such as user actions, I/O signals, or messages from other programs. Event-driven programming (EDP) is the prevalent paradigm for graphical user interfaces, web clients, and it is rapidly gaining importance for server-side and network programming. For instance, the HTML5 standard mandates that user agents be implemented using EDP. Likewise, widely used frameworks such as Node.js, memcached, and Nginx rely on EDP.

In EDP, each program has an *event loop* which consists of a FIFO queue and a control process (or thread) that listens to events. Events that arrive are pushed into the queue and are sequentially dispatched by the control process according to a FIFO policy. A key feature of EDP is that high-latency operations, such as database or network requests, can be handled asynchronously: They appear in the queue only as events signaling start and completion, whereas the blocking operation itself is handled elsewhere. In this way EDP achieves the responsiveness and fine-grained concurrency required for modern user interfaces and network servers, without burdening programmers with explicit concurrency control.

Our recent research shows that there is a downside to EDP-based systems, namely, that they are susceptible to side-channel attacks. The key observation is that event loops form a resource that can be shared between mutually distrusting programs. Hence, contention of this resource by one program can be observed by the others through variations in the time the control process takes for dispatching their events. Specifically, we exhibit attacks against the two central event loops in Google's Chrome web browser: that of the I/O thread of the host process, which multiplexes all network events and user actions, and that of the main thread of the renderer processes, which handles rendering and Javascript tasks.

For each of these loops, we show how the usage pattern can be monitored with high resolution and low overhead, and how this can be abused for malicious purposes, such as web page identification, user behavior detection, and covert communication. Our results point to fundamental security and privacy issues in the event-driven architecture of browsers that need to be addressed in a fundamental manner.

The paper describing our work has received a *Distinguished Paper Award* at the USENIX Security Symposium, one of the premier venues for security research.

Related publications

[1] P. Vila and B. Köpf. Loophole: Timing Attacks Against Shared Event Loops in Chrome. In *26th USENIX Security Symposium*, 2017.

editor
imdea software institute

graphic design
base 12 diseño y comunicación

photos on pages 13, 14, 75 and 97
Daniel Schäfer

legal deposit number
M-7080-2018