José Fragoso Santos

INESC-ID
Av. Rovisco Pais, 1
+351 915790280
jose.fragoso@tecnico.ulisboa.pt
j3fsantos
https://j3fsantos.github.io

Profile & Goals My long-term research goal is to establish a certified infrastructure and a principled methodology for developing scalable sound program analyses for dynamic languages. My method is to combine deep theoretical results with tool building for verification of real-world software. My expertise spans a wide range of approaches to program analysis and verification: symbolic execution, separation logics, type systems, information flow control, compiler construction.

Current position

Sep 2019–present **Assistant Professor**, DEI, *Instituto Superior Técnico, Universidade de Lisboa*, Portugal

Experience

Mar 2015–Aug 2019 **Research Associate**, Department of Computing, *Imperial College London*, UK

Topic Specification, verification, and testing of JavaScript programs.

Project Certified Verification of Client-Side Web Programs, EPSRC Grant, Reference EP/K032089/1
REMS: Rigorous Engineering for Mainstream Systems, EPSRC Grant, Reference EP/K008528/1

Supervisor Philippa Gardner

Aug 2009–Sep 2010 **Research Assistant**, SQIG,
Instituto de Telecomunicações, Portugal

Topic Flexible information flow control.

Project KLog: Logics for Security.

Supervisor Ana Almeida Matos

Jan 2009–Aug 2009 **Research Assistant**, Vision Laboratory,
Institute for Systems and Robotics, Portugal

Topic Automatic self-calibration of a humanoid's robot head.

Project BIO-LOOK: Biomimetic Oculomotor Control for Humanoid Robots.

Supervisor Alexandre Bernardino

Oct 2007–Nov 2008 **Research Assistant**, *SAT Group*, INESC ID

Topic Learning techniques for pseudo-boolean optimisation and solving.

Project BSOLO: Pseudo-Boolean Solving and Optimisation

Supervisor Vasco Manquinho

Education

2011–2014 **PhD in Computer Science**, *University of Nice Sophia Antipolis*, France

Thesis Enforcing Secure Information Flow in Client-Side Web Applications

Supervisor Tamara Rezk and Ana Almeida Matos

Jury David Naumann (Stevens Institute of Technology), Peter Thiemann (Univ. of Freiburg), Cédric Fournet (Microsoft Research), and Vasco Vasconcelos (Univ. of Lisbon).

2006–2008 **M.Sc. in Information Systems and Computer Engineering**,
Instituto Superior Técnico, Portugal, 18/20

Thesis Learning Techniques for Pseudo-boolean Solving and Optimisation

Supervisor Vasco Manquinho

Jury Inês Lynce (IST), Vasco Manquinho (IST), Nuno Mamede (IST)

2003–2006 **B.Sc. in Information Systems and Computer Engineering**,
Instituto Superior Técnico, Portugal, 16/20

Awards

2018 **Winner of the Research Award on Continuous Reasoning Research**,
Facebook, UK (together with Philippa Gardner and Petar Maksimović)
50K USD for furthering my work on JaVerT 2.0.

2011–2014 **FCT PhD Scholarship**, *Fundação para a Ciência e Tecnologia*, Portugal
Fully-funded PhD scholarship.

Publications

My research output is characterised by high-quality papers in top-tier conferences.
Total citations 95 h-index 6 (Google Scholar, Jan 2019).
CORE rank: 2 × **A***, 2 × **A**, 4 × **B**

POPL'19 **JaVerT 2.0: Compositional Symbolic Execution for JavaScript**,
J. Fragoso Santos, P. Maksimović, G. Sampaio and P. Gardner.
In Proc. of Symposium on Principles of Programming Languages. ACM SIGPLAN. 2019.
Citations 3 CORE rank A* Length 31 pages

PPDP'18 **Symbolic Execution for JavaScript**,
J. Fragoso Santos, P. Maksimović, T. Grohens, J. Dolby, P. Gardner.
In Proc. of Symposium on Principles and Practice of Declarative Programming.
ACM. 2018.
Citations 3 CORE rank B Length 14 pages

POPL'18 **JaVerT: JavaScript Verification Toolchain**,
J. Fragoso Santos, P. Maksimović, D. Naudžiūnienė, T. Wood, and P. Gardner.
In Proc. of Symposium on Principles of Programming Languages. ACM SIGPLAN. 2018.
Citations 15 CORE rank A* Length 33 pages

CADE'17 **Towards Logic-Based Verification of JavaScript Programs**,
J. Fragoso Santos, P. Gardner, P. Maksimović, and D. Naudžiūnienė.
In Proc. of International Conference on Automated Deduction.
Vol. 10395 of LNCS. Springer. 2017.
Citations 3 CORE rank A Length 18 pages

APLAS'16 **DOM: Specification and Client Reasoning**,
A. Raad, J. Fragoso Santos, P. Gardner.
In Proc. of Asian Symposium on Programming Languages and Systems.
Vol. 10017 of LNCS. Springer. 2016.
Citations 6 CORE rank B Length 20 pages

JCS'16 **Mashic Compiler: Mashup Sandboxing based on Inter- frame Communication**,
Z. Luo, J. Fragoso Santos, A. A. Matos, T. Rezk.
In Journal of Computer Security. ACM. 2016.
Citations 1 CORE rank B Length 45 pages

TGC'15-2 **Modular Monitor Extensions for Information Flow Security in JavaScript**,
J. Fragoso Santos, T. Rezk, A. Almeida Matos.
In Proc. of Symposium on Trustworthy Global Computing.
Vol. 9533 of LNCS. Springer. 2015.
Citations 0 CORE rank - Length 13 pages

TGC'15-1 **Hybrid Typing of Secure Information Flow in a JavaScript- like Language**,
J. Fragoso Santos, T. Jensen, T. Rezk, A. Schmitt.
In Proc. of Symposium on Trustworthy Global Computing.
Vol. 9533 of LNCS. Springer. 2015.
Citations 5 CORE rank - Length 13 pages

TGC'14 **An Information Flow Monitor for a Core of DOM - Introducing References and Live Primitives**,
A. Almeida Matos, J. Fragoso Santos, T. Rezk.
In Proc. of Symposium on Trustworthy Global Computing.
Vol. 8902 of LNCS. Springer. 2014.
Citations 8 CORE rank - Length 15 pages

SEC'14 **An Information Flow Monitor-inlining Compiler for Securing a Core of JavaScript**,
J. Fragoso Santos, T. Rezk.
In Proc. of IFIP International Information Security and Privacy Conference.
Springer. 2014.
Citations 28 CORE rank B Length 16 pages

PLAS'12 **Typing Illegal Information Flows as Program Effects**,
A. Almeida Matos, J. Fragoso Santos.
In Proc. of Workshop on Programming Languages and Analysis for Security. ACM. 2012.
Citations 6 CORE rank - Length 12 pages

IROS'10 **Sensor Based Self Calibration of the iCub's Head**,
J. Fragoso Santos, A. Bernardino, J. Santos-Victor.
In Proc. of International Conference on Intelligent Robots and Systems. IEEE. 2010.
Citations 8 CORE rank A Length 12 pages

IWIL'08 **Learning Techniques for Pseudo-Boolean Solving**,
J. Fragoso Santos, V. Manquinho.
In Proc. of International Workshop on the Implementation of Logics. CEUR-WS.org. 2008.
Citations 4 CORE rank - Length 10 pages

Teaching

2015/2018 **Course Support Leader** of Separation Logic (4th year course),
Imperial College London, UK
Leader of teaching assistants

Duties Assist the lecturer in preparing tutorial sheets, coursework and lecture notes; mark coursework; give tutorials.

PhD and Project supervision

2017–ongoing Assistant Supervisor of **Gabriela Sampaio**, PhD in Computer Science, *Imperial College*
Topic Automatic Reasoning about DOM Events using JaVerT.

2018–2019 **Eric Wenhao Ruan Zhu**, MEng Joint Mathematics and Computing, *Imperial College London*
Topic Multi-theory First Order Solver for Program Analysis and Verification.
Mark 78/100

2018–2019 **Priyanka Shah**, MEng Computing, *Imperial College London*
Topic Compiling JavaScript Regular Expressions.
Mark 75/100

2018–2019 **Si Wei Tan**, MEng Computing, *Imperial College London*
Topic Trusted Infrastructure for JavaScript (ES5) Analysis.
Mark 90/100, *IBM Project Prize*

2017–2018 **Radu-Andrei Szasz**, MEng Computing, *Imperial College London*
Topic Typing JavaScript Through Symbolic Execution.
Mark 90/100, *IBM Project Prize*

2017–2018 **Beatrix de Wilde**, MEng Computing, *Imperial College London*
Topic Towards Automatic Verification of JavaScript Programs.
Mark 86/100

2017–2018 **Cesar Roux Dit Buisson**, MEng Computing, *Imperial College London*
Topic Web of Truths: Formal Verification of JavaScript DOM Clients.
Mark 82/100

2017–2018 **Iván Matellanes**, MSc Computing, *Imperial College London*
Topic A Verification Tool for JavaScript.
Mark 82/100

Interns

Summer 2018 **Emma Tye**, 2nd year research internship, *Imperial College London*
Topic Verifying AVL-tree algorithms using JaVerT 2.0.

Spring 2018 **Théotime Grohens**, Final year research internship, *Imperial College London*
Topic Symbolically testing real-world JavaScript libraries.

Summer 2017 **Thomas Pointon**, 1st year research internship, *Imperial College London*
Topic Verifying doubly-linked list algorithms using JaVerT.

Invited Talks

Jun 2017 Invited talk at **JSTools'17**, Barcelona, Spain
Invitation-only seminar organised by J. Dolby and C. Hammer co-located with ECOOP'17.
Topic *JaVerT: a Logic-based Tool for JavaScript Verification*

Jun 2016 Invited talk at **JSTools'16**, Rome, Italy
Invitation-only seminar organised by J. Dolby and C. Hammer co-located with ECOOP'16.
Topic *Toward Logic-based Verification for JavaScript*

Apr 2012 Invited talk at **the 19th Crest Open Workshop on Interference and Dependence (COWL)**, London, UK
Invitation-only seminar organised by the Department of Computer Science at UCL.
Topic *Typing Illegal Information Flows as Program Effects*

Research Talks

JaVerT 2.0: Compositional Symbolic Execution for JavaScript

Jan 2019 POPL'19, Lisbon, Portugal.
Dec 2018 Departamento de Informática, Faculdade de Ciências, Lisbon, Portugal.
Hosted by Vasco Vasconcelos.
Dec 2018 Departamento de Engenharia Informática, IST, Lisbon, Portugal.
Hosted by José Carlos Monteiro.

Symbolic Execution for JavaScript

Sep 2018 PPDP'18, Frankfurt, Germany.

JaVerT: JavaScript Verification Toolchain

Jan 2018 POPL'18, Los Angeles, USA.
Dec 2017 Systems Security Group, Royal Holloway University, London, UK.
Hosted by Johannes Kinder.
Dec 2017 NOVA LINCS, Lisbon.
Hosted by Carla Ferreira.

Hybrid Typing of Secure Information Flow in a JavaScript-like Language

Sep 2015 TGC'15, Madrid, Spain.

Modular Monitor Extensions for Information Flow Security in JavaScript

Sep 2015 TGC'15, Madrid, Spain.

Enforcing Secure Information Flow in Client-Side Web Applications

Nov 2014 LAFHIS Research Lab, University of Buenos Aires, Buenos Aires, Argentina.
Hosted by Viktor Braberman.
Nov 2014 LoReL Group, Universidad Nacional de Quilmes, Quilmes, Argentina.
Hosted by Eduardo Bonelli.
Nov 2014 FaMAF, Universidad Nacional de Córdoba, Córdoba, Argentina.
Hosted by Pedro D'Argenio.

An Information Flow Monitor for a Core of DOM - Introducing references and live primitives

Oct 2014 Department of Computing, Imperial College London.
Hosted by Sergio Maffeis.
Sep 2014 TGC'14, Rome, Italy.

An IFlow Monitor-inlining Compiler for Securing a Core of JavaScript

Jun 2014 SEC'14, Marrakech, Morocco.

Typing Illegal Information Flows as Program Effects

Jun 2012 PLAS'12, Beijing, China.

Sensor Based Self Calibration of the iCub's Head

Nov 2010 IROS'10, Taipei, Taiwan.

Learning Techniques for Pseudo-Boolean Solving

Nov 2008 IWIL'08, Doha, Qatar.

Academic Activities

Reviewer *Conferences:* CSF 2012, PLAS 2013, LATIN CRYPT 2013, CSF 2014, POST 2014, POPL 2017, CSF 2018.
Journals: Journal of Computer Security.

Research Software

JaVerT 2.0 A JavaScript program analysis tool with support for: whole-program symbolic testing, semi-automatic separation-logic-based verification, and fully-automatic compositional testing. (With P. Maksimović).

– A novel combination of symbolic execution with compositional program reasoning based on separation logic.

Website `https://github.com/javert2/JaVerT2.0/`

– Used by Peter Thiemann at the University of Freiburg.

Cosette A tool for general-purpose whole-program symbolic testing of JavaScript programs. (With J. Dolby, T. Grohens, and P. Maksimović).

JaVerT The first separation-logic-based verification tool for JavaScript.
(With P. Maksimović, D. Naudžiūnienė, and T. Wood).

– It comprises: JS-2-JSIL, a thoroughly tested compiler from JavaScript to JSIL; JSIL Verify, a separation-logic-based verification tool for JSIL; and axiomatic specifications of the JavaScript internal functions.

Mashic A mashup compiler for automatic sandboxing of third-party JavaScript code.
(with A. Almeida Matos, Z. Luo, and T. Rezk).

Website `http://web.ist.utl.pt/~ana.matos/Mashic/mashic.html`

Industrial Outreach

Mar 2018 Represented Imperial College London at the **official meeting of the ECMA TC39**, the ECMAScript international committee. London, UK.

Research Visits

Nov 2018 Visited the Flow Team at **Facebook**. Menlo Park, California, USA.

Jan 2018 Visited **Galois**. Portland, Oregon, USA.

Jan 2018 Visited the Hack Team at **Facebook**. London, UK.

Other skills

Languages Portuguese (native speaker) • English (full professional proficiency) • French (fluent)

Programming OCaml, Racket, JavaScript, Java, C, C++.