Information and Communication Technologies Institute

Carnegie Mellon | PORTUGAL

AN INTERNATIONAL PARTNERSHIP

Certified INTERFACES for Integrity and Security in Extensible Web-based Applications

Authors:
Luís Caires,
Frank Pfenning,
António Melo,
João Seco,
Vasco Vasconcelos

Start Date: 1/5/2009
End Date: 30/4/2012
Actual End Date: 31/12/2012
(8 months no cost extension)

Final Report (June 10, 2013)

Project Reference (FCT):
NGN 44 - 2009-2012

Subject: Final Report of the Research Project
This document extends the Y1-2 interim reports and summarizes project results.

Project Review Meeting 2013

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

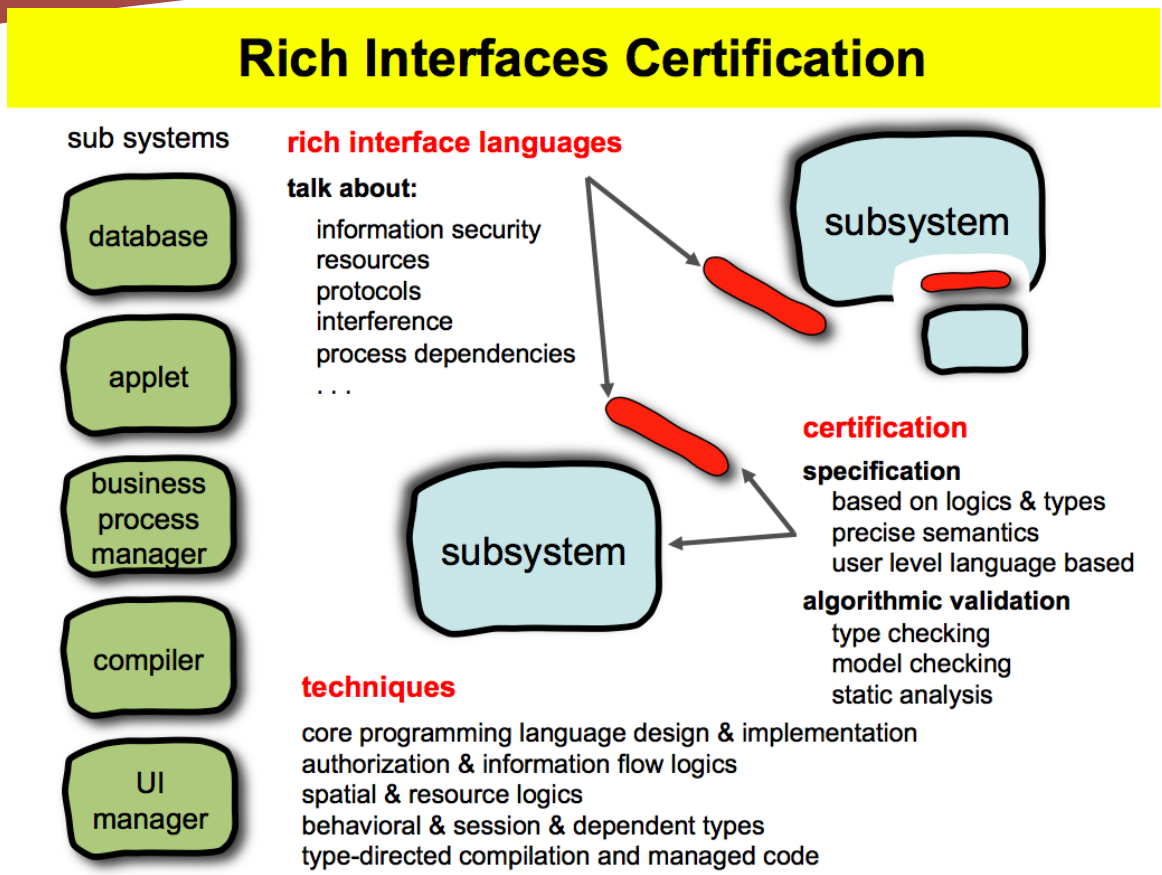
Contents

1. Abstract (300 words)

[Reproduced from Y1-Y2 interim reports.
Section 13 offers a description of INTERFACES aimed for the general public]
The increasing availability of Internet-based services and of various sorts of devices with substantial computing and networking abilities is contributing to the growth of a global software service-based infrastructure upon which the general society is becoming more and more dependent. This computing infrastructure is under permanent extension and active modification by parties working independently, even if it must support critical businesses and activities.

Project INTERFACES targets the development of new techniques and tools for enforcing security, integrity, and correctness requirements on distributed extensible web-based applications by introducing novel, semantically rich notions of interface description languages, based on advanced type systems and logics.

Key outputs of the INTERFACES approach will be core typed programming languages and environments for building extensible certified web applications, as well as design and implementations of prototypes for specification, programming, and reasoning about case studies, in collaboration wih the industrial parner OutSystems SA, developer of the Agile Platform, a widely used web-based application development environment.



2. Table of PIs/ Co-PIs information

University	Name	Title	Contact Info	% In Project
CSD Carnegie Mellon University	Frank Pfenning (PI)	Full Professor	fp@cs.cmu.edu http://www.cs.cmu.edu/~fp/	
DI FCTUNL (CITI)	Luís Caires (PI)	Full Professor	luis.caires@di.fct.unl.pt http://ctp.di.fct.unl.pt/~lcaires	
DI FCUL (LASIGE)	Vasco Vasconcelos (Co-PI)	Full Professor	vv@di.fc.ul.pt http://www.di.fc.ul.pt/~vv/	
OutSystems SA www.outsystems.com	António Melo (Co-PI)	VP Engineering	antonio.melo@outsystems.com	

3. Table of Staff, Post-docs, Students, Company Collaborators

University	Name	Title	Contact Info	% In Project
DI FCTUNL (CITI)	João Costa Seco	Assistant Professor		
	Carla Ferreira	Assistant Professor		
	Jorge Perez	PostDoc (April 2010, present) (PhD sup Davide Sangiorgi, U. Bologna, 2009)		
	Hugo T. Vieira	Assistant Professor (until October 2012)		
	Bernardo Toninho	PhD Student (Dual Degree CMU CS, joined Fall 2009)(*)		
	Filipe Militão	PhD Student (Dual Degree CMU CS, joined Fall 2009)(*)		
	Luísa Lourenço	PhD Student (UNL)		
	Mário Pires	PhD Student (UNL)		
	Miguel Domingues	PhD Student (UNL)		
CSD Carnegie Mellon University	Bernardo Toninho	PhD Student (Dual Degree CMU CS, joined Fall 2009)(*)		
	Filipe Militão	PhD Student (Dual Degree CMU CS, joined Fall 2009)(*)		
	Jason Reed	PhD Student (until August 2009)		
	Robert Simmons	PhD Student (since September 2010)		
	William Lovas	(partial support September 2009 to August 2010)		
DI FCUL (LASIGE)	Francisco Martins	Assistant Professor		
	Hugo T. Vieira	Assistant Professor (from October 2012 on)		
	Pedro Baltazar	PostDoc (Feb 2011, Dec 2011) (PhD sup Paulo Mateus, IST, 2010)		
	Kohei Suenega	PostDoc (April 2010, Jan 2011) (PhD sup Naoki Kobayashi, U.Tokyo, 2008)		
	Alexandre Zua Caldeira	PhD Student (FCUL)		
OutSystems SA	Lúcio Ferrão	Chief Software Architect		
	Gonçalo Borrega	R&D Platform Manager		
	Several other members of the R&D and Product management team			

4. Research Questions

The increasing availability of Internet-based services and of various sorts of devices with substantial computing and networking abilities is contributing to the growth of a global software service-based infrastructure upon which the general society is becoming more and more dependent. This computing infrastructure is under permanent extension and active modification by parties working independently, even if it must support critical businesses and activities.

Among the most successful applications built on this infrastructure one finds particularly critical services, such as those that need to securely exchange information with previously unknown parties (for example, web portals), and applications willing to modify or extend their functionality in a trustworthy and reliable way, without interrupting operation (for example, a web browser). We also find applications that need to exchange not only data but also executable programs (either in the form of compiled code or in the form of other interpretable specifications, such as XML descriptions), and to reconfigure themselves in order to select and bind to suitable partners, a kind of behavior present in service oriented systems, such as those based on web-service technology. Common instances of extensible network-based applications include complex, reconfigurable applications such as enterprise information systems, required to evolve at the rapid pace that today's businesses need, and even general purpose devices such as mobile phones and PDAs, that keep increasing their computational capabilities everyday. Enforcing security, integrity and correctness requirements in such open and extensible application scenarios raises many challenges.

How can we combine runtime monitoring with static analysis of code when programs run on multiple, possibly untrusted environments? How would it be possible to validate that dynamic updates to running applications will not violate the prescribed security and integrity constraints? How can we guarantee that a web-service collaboration does not violate the intended message interaction sequence, as defined by previously agreed business protocols, or does not exceed reasonable bounds on resource usage, as prescribed by a service level agreement? How can we guarantee that developers of a complex web application do not inadvertently violate security policies, allowing untrusted users to access private data? How can we make sure that the mechanisms made available for allowing the execution of foreign code will not open the door to virus infections? How can we incorporate in programming languages, analysis tools, and execution infrastructures, proof procedures and algorithms able to certify properties far beyond the usual type safety, such as secrecy, authenticity, concurrency control, access control, and conformance to protocols? In general terms, how can we define, in mathematical precise ways, the expectations and requirements of software fragments, so that software developers may determine as early as possible, ideally at compile or link time, that combinations will not break the intended key integrity constraints?

Although some of the mentioned issues have been addressed by several research directions, a distinguishing challenge placed to INTERFACES is to cope with the highly dynamic and “live” character of agile software development for web apps, where not only

static aspects but also dynamic aspects (e.g., the state, self-healing) must be taken into account in order to keep the integrity of the running system integrity, in a context where practical usability is also an important concern. INTERFACES will approach these challenges by developing new notions of semantically rich interface languages, and associated type and logic based verification techniques. Such interface languages must contain fragments easily understandable by software developers / engineers, be expressive enough to specify relevant properties of subsystems, and support reasonable efficient algorithms to certify that components conform to their published interface specifications.

A key output of the INTERFACES approach will be core typed programming languages and environments for building extensible certified web applications, including prototype implementation, useful for validations and demonstration purposes. Other expected scientific results include:

- Define logic and type based interface languages for describing security and integrity properties of distributed extensible applications or services on the Internet.

- Develop programming models and languages supporting logic and type-based rich interface languages, amenable to formal analysis, based on type checking / model-checking, in the context of high-level specifications of integrity and security.

- Produce implementations of prototypes for specification, programming, and reasoning about case studies, including scenarios provided by an industrial strength web-based application development environment, the OutSystems Service Studio and Platform.

5. Scientific Progress and Accomplishments

In the initial proposal, project tasks were organized around four interrelated research threads, three more foundational tasks ("Interfaces for Security", "Interfaces for Resources and Behavior", "Interfaces for Disciplining Communication"), addressing the key properties of components which we seek to expose in interfaces and their associated analysis and verification techniques, and a fourth task "Validation" focusing on integration, implementation, and validation. However, in this project we aim to both successfully deliver (1) frontier research results, able to sustain the challenges and requirements of the field and motivate PhD level research work, and (2) developmental work needed not only for validating the approaches in scenarios of real industrial significance, with an eye on technology transfer, but also for dissemination and demonstration purposes. Achieving these goals demands careful planning and articulation between activities and interactions between the several partners and tasks.

During Y1-Y2 INTERFACES strived to refine the project scientific work breakdown organization, setting up several horizontal activities between the four parallel themes mentioned above, so to increase the effectiveness of collaborations, and aiming to promote global collaboration and optimize and focus the contributions of each partner, whose research competencies range from the theoretical underpinnings, to the implementation of runtime infrastructures, and even usability concerns. Based on the Y1

experience, we stabilized the research approach on four interacting layers (Foundations / Core Language / Validation / Demonstrators), which crosscut the above mentioned focus themes of "Security", "Resource-Behavior" and "Communication", approach that we continued to follow during Y2-Y3. A key component of the INTERFACES methodological approach is the development of a core programming language and environment for extensible certified web applications and associated language and type based verification techniques, including prototype/demonstrable implementation.

Both foundational results/techniques and requirements/challenges raised by real needs of agile web application development influence and are influenced by the development of the core system, which will be used as a test bed for INTERFACES developed concepts and techniques. All partners are collaborated in the design of the core programming language / environment, which is a distillation of the OutSystems DSL, and associated prototypes. Several interface languages and associated validation techniques to describe security, composability, resource usage, communication protocols, and dynamic reconfiguration are investigated. The current prototype of the INTERFACES certified web application development environment (LiveWeb), together with its theoretical underpinnings and associated fundamental techniques, will contimue to be the running demonstrable of our project. Latest upgrades include support for dynamic reconfiguration and information flow analysis of data manipulation language.

We now summarize specific scientific results obtained by the team in Y1–Y3 that relate to the general goals described above.

Logical Foundations for Distributed Session Types

New foundations for session-based communication, ensuring fidelity and absence of deadlocks in service protocols, based on interface contracts described in propositional linear logic and dependently typed linear logic. This work has caught considerable attention by the community (see citations and eg. Philip Wadler's talk at Milner Symposium), as it provides the first purely logical explanation (in the sense of Curry-Howard) of sophisticated (yet practical) interface contracts for distributed communication, and already motivated several extensions. Recent contributions of this line of work are developed in the context of Toninho's PhD thesis (expected 2014).

Closely related references [8,24,23,30,31,35,37,41].

Security Verification of Data-Centric Web Applications

Techniques to specify and validate via (type based static analysis and dynamic checks) security policies in distributed web applications, including policies related to authorization and access control to data stored in relational databases, possibly allowing a compiler to detect potentially unsecure database manipulation code.

Closely related references [13, 22, 27, 34, 43, 55, 60, 63, 64, 65, 57].

Role Based Validation of Data Security in the OutSystems SA Service Studio

A prototype for model-driven data role-based security, implemented as a dynamically

validated version of the work described above, was developed by OuySystems in a branch of the OutSystems Service Studio development tree. Another major outcome of Y3 on this line of research is the submission (joint OutSystems / UNL) of a US Patent, based on the same work, but extending it with a generalization of the standard RBAC model with so-called data-roles.

Closely related references [22, 27, 48, 51, 66].

Certification of Distributed Interface Contracts

Validation techniques, based in linear logic type systems, to enforce interface contracts in distributed web applications, including the enforcement of properties of communicated data. In this line of work, we exploit simple logical mechanisms to express data integrity, behavioral and causality constraints, trust, higher-order (mobile) code, proof carrying code, dynamic reconfiguration, and even termination.

Closely related references [7,14,28, 30, 31, 34, 37, 38, 41, 42].

Multiparty Distributed Sessions

Validation techniques, based in type systems, to enforce the coordination of message-based communications between several participants in web-service based collaborations, based on conversation types. Recently published work (joint FCTUNL- FCUL) investigated how to dynamically map roles into the various parties collaborating in a business process.

Closely related references [2,10,18, 29, 33, 39, 45, 57].

Web Programming Language and Environment Design and Implementation

Design and analysis of several core DSLs for web application development where produced, as well several techniques for their implementation and optimization. Some of the techniques investigated where actually implemented on the OutSystems platform. Ongoing work now focuses on the security and module definition layers.

Closely related references [15, 32, 39, 44, 45, 46, 47, 56, 59, 60, 61, 63].

Core Language and Development Environment Prototypes

New version of the INTERFACES core language and prototype started during Y1-Y2 were produced in Y3. The current prototype demonstrates static (compile time) verification of data security and static (link time) validation of mashups (the dynamic integration of pieces of a web page, originating from possibly untrusted parties) based on refinement types, and information flow analysis of data manipulation (sql-like) operations. The verifier builds on SMT solving.

Closely related references [22, 27, 43, 61, 63, 64, 65, 67].

Verification of Concurrent Programs

Validation techniques, based on core programming languages and type systems, to

discipline concurrency in object-oriented programs have been developed, focusing on the static verification that objects in a software system are used by clients according to the declared protocols (for example, a business process), a minimal condition for system integrity. We have considered both in memory objects and distributed objects, and safety and liveness properties (e.g., race absence / deadlock). A recent highlight in this line of research is our POPL'13 paper on behavioral separation types.

Closely related references [1, 3, 9, 11, 12, 16, 17, 19, 26, 40].

Reasoning Frameworks

Communication patterns of distributed systems can be described in propositional linear logic, as we have shown in [24]. A dependent logical framework may then provide basic mechanisms by which such extensions can be designed. Several advances on the fundamental logical and process algebraic reasoning mechanisms, useful for checking interface properties have been developed.

Closely related references [4, 5, 14, 19, 21, 25, 35, 36, 53, 54].

6. Interactions

Key interactions

- FCTUNL/OutSystems SA: Routine Meetings (OutSystems SA headquarters, roughly once a week in Y1-Y2, thrice a month Y3). At major milestones, oral reports have been presented to groups of selected members of OutSystems engineering team.
- Research visit from FCTUNL (Caires) to CMU (February 2009).
- Research visit from CMU (Pfenning) to FCTUNL /FCUL (February 2009)
- FCTUNL/OutSystems SA/CMU/FCUL: kickoff meeting (OutSystems headquarters), February 2009.
- INTERFACES workshop involving FCTUNL and FCUL featuring a talk by by Aldrich at CITI FCT UNL on "Typestate Verification for Aliased Objects using Invariant-Carrying Permissions" (July 2009).
- Research visit from FCTUNL/FCUL (Caires/Vasconcelos) to CMU (May 2010).
- Research visit from CMU (Pfenning) to FCTUNL/FCUL (February 2010).
- FCTUNL/OutSystems SA/CMU/FCUL: General Meeting (with all the team, included hired postdocs), May 2010. CMU participated by videoconference.
- Caires and Vasconcelos attended a CMU|Portugal Aerminium Project Workshop at Carnegie Mellon University, and delivered lightening talks (May 2010).

- Research visit from FCTUNL/FCUL (Caires/Seco) to CMU (April 2011).
- UNL researcher Carla Ferreira participated in the Faculty Exchange Program between January 2011 and July 2011. The main goal was to start a new research direction on information flow analysis for higher order imperative programs. Researchers currently involved in this line of work are Ferreira, Caires, Seco and Pfenning.
- An international workshop, co-sponsored by INTERFACES, joined at FCT UNL more than 40 key researchers in the field, from all over the world, discussed the state of the art in type-based analysis of software systems behavior. Program and attendee listing can be consulted a: http://www.dcs.gla.ac.uk/~simon/BehaviouralTypes/
- Research visit from CMU (Pfenning and Aldrich) to UNL and FCUL (April 2011).
- Research visit from CMU (Pfenning) to UNL (October 2011).
- Joint Aeminium/INTERFACES workshop involving FCTUC, FCTUNL, FCUL, UMA and Carnegie Mellon University, featuring talks by academic and industrial partners (Novabase / Outsystems), at the Reitoria UNL, to be held November 9, 2011. This workshop exploits synergies between the two Carnegie Mellon Portugal projects AEMINIUM and INTERFACES, both developing programming language techniques even if with different focus and goals. Caires, Aldrich and Marques have been collaborating around the co-supervision of INTERFACES and AEMINIUM PhD students Filipe Militão and Sven Stork.
- Carla Ferreira visited CMU from January to August 2012 in the faculty exchange program with two complementary goals: a research collaboration with Frank Pfenning on combining refinement types and information flow types. The work extended previous research developed within Interfaces project, namely on lambda-db, a typeful language for defining access control policies in data centric systems.
- João Costa Seco visited Carnegie Mellon University from August 21 to December 21, 2012 to work with Frank Pfenning, also with a Fellowship from the Carnegie Mellon Portugal, Faculty Exchange Program. The main goal of this visit was to continue and extend the work started by Carla Ferreira in a previous visit on the foundations of type based security and imperative languages. This line of work has led to [63], and influenced the development of the 3rd version of the Liveweb prototype [67]. A publication targeting a top venue is under preparation.
- Toninho, Militão, Caires and Perez visited CMU. Caires delivered a PoP seminar. Several research meetings related to INTERFACES research issues (May 2012).
- Aldrich visited UNL, for research meetings with Militão and Caires (June 2012).
- Simon Gay e Nils Gesbert, University of Glasgow, Reino Unido. Visit to FCUL to discuss behavioral interfaces with the INTERFACES team (September 2012).
- Frequent routine VC interactions between UNL and CMU, related to the supervision of our Dual Degree PhD students.

Several talks by INTERFACES researchers, in which several team members from various partner institutions have attended (see Publications section).

Involvement of PhD students

- Bernardo Toninho (co-supervisors Pfenning/Caires, CMU|PT fellowship), started Fall 2009, first semester at FCT UNL, second semester at CMU. Academic years 2010 / 11 at CMU. Thesis Proposal expected 2013.
- Jason Reed at Carnegie Mellon University (supervisor Pfenning).
- Filipe Militão (co-supervisors Caires/Aldrich, CMU|PT fellowship), started Fall 2009, first year at CMU. Academic year 2010/11 at UNL. Thesis Proposal expected 2013.
- Robert Simmons at Carnegie Mellon University (supervisor Pfenning).
- Alexandre Zua Caldeira at FCUL (ongoing, supervisor Vasconcelos, FCT MCTES fellowship).
- Luísa Lourenço at UNL (ongoing, supervisor Caires, FC&T MCTES fellowship)
- Miguel Domingues at UNL (ongoing, supervisor Seco, FC&T MCTES fellowship)

Recruitment

During Y1, INTERFACES has recruited two post-doc researchers: Jorge Perez and Kohei Suenaga. Positions were opened even before the project contract was officially signed. The call (closed 15 October) attracted 10 international applications (1 Portugal, 3 Italy, 1 USA, 1 Japan, 1 France, 1 Jordan, 1 Lithuania, 1 Spain).

The selection process was concluded by the end of the year, but due to administrative / re-locating / visa reasons, the contracts were only enabled from April 2010. Perez was located at CITI FCTUNL, and Suenaga at LASIGE FCUL.

Suenaga left for a position at Kyoto University Japan by the end of December 2010.

A replacement position was open, which attracted 5 international applications (1 Brazil, 1 Italy, 1 UK, 1 Portugal, 1 France). Pedro Baltazar was selected, and assigned to the LASIGE FCUL pole. Pedro Baltazar postdoctoral fellowship terminated December 2012.

Jorge Perez has continued his activities at the FCT UNL pole during Y3. He is now still working at UNL, under a FC&T MEC post-doctoral fellowship.

One assistant researcher (Miguel Lourenço) was partially hired by the project during Y3, now supported by a FC&T MEC doctoral fellowship.

7. Milestones, Deliverables, and Achievements

The preliminary milestones scheduled for Y1 and Y2 have been achieved. (see previous reports) The preliminary milestones scheduled for Y3 have been mostly achieved as well, as we have demonstrated in the previous sections of this report.

INTERFACES initial statement of work for Y3 was the following:

Year 3

• Second prototype of logical policy analysis tools and validation against realistic security policies in industry.

• Demonstration of information flow enforcement through a combination of static and dynamic techniques based on epistemic logic.

• Interfaces, based on combination of static typing, dynamic typing, and proof checking, for enforcing safety of dynamic updates and self-healing in running web applications.

• Session and behavioral type based approaches for life-cycle control, concurrency control, and separation of duties in business workflows.

• Incorporation of the developed interface languages and related verification techniques in the core programming language and environment, for validation and dissemination purposes, including implementation of validation algorithms in the prototype.

The preliminary milestones scheduled for Y3 have been mostly achieved as well, with minor adjustments, as we have demonstrated in the previous sections of this report. The first two topics focused mostly on data security.

Summary of Research Outputs

Type of Output	Number
Journal Papers	8
Conference Papers (peer reviewed)	31
Reports	7
Patents (pending)	1
PhD Students involved	6
PhD Thesis	2
MSc Thesis	10
Prototypes (includes versions)	4
Presentations	35
Press Releases	6

The prior interim reviews made by the evaluation panels rated the project with an overall grading of “Excellent”.

8. Publications and Presentations

8.1. Number of peer reviewed papers published in Journals

8

8.2. List of peer reviewed papers published in Journals

1. Simon Gay and Vasco T. Vasconcelos. ***Linear type theory for asynchronous session types***. Journal of Functional Programming, 20(1), Cambridge, 2010.

2. Luís Caires and Hugo T. Vieira. ***Conversation Types***. Theoretical Computer Science, 411(51-52), 4399-4440, Elsevier, 2010.

3. Vasco T. Vasconcelos. **Sessions, from types to programming languages**. Bulletin of the European Association for Theoretical Computer Science, 103:53–73, 2011.

4. Ivan Lanese, Jorge A. Pérez, Davide Sangiorgi, Alan Schmitt: **On the expressiveness and decidability of higher-order process calculi**. Information and Computation 209(2): 198-226, Elsevier, 2011.

5. Robert J. Simmons and Frank Pfenning. **Logical approximation for program analysis**. Higher-Order and Symbolic Computation, Springer-Verlag, 2011.

6*. Vasco T. Vasconcelos. **Fundamentals of Session Types**. Information and Computation, 217:52–70, 2012.

7*. Mario Bravetti, Cinzia Di Giusto, Jorge A. Pérez, Gianluigi Zavattaro: **Adaptable Processes**. Logical Methods in Computer Science 8(4) (2012).

8*. Luís Caires, Frank Pfenning and Bernardo Toninho. **Session Types as Linear Logic Propositions**. Mathematical Structures in Computer Science, Cambridge UP, to appear 2013.

9.3. Number of peer-reviewed conference papers published

31 + 4 papers produced within the project but published after 31-12-12

9.4. List of peer-reviewed conference papers published

9. Filipe Militão and Luís Caires. ***An Exception Aware Behavioral Type System for Object-Oriented Programs***. INFORUM 2009, Actas do Symposium de Informática. Lisboa, Portugal, 2009. Best Student Paper Award (BES Award 2009).

10. Luís Caires and Hugo T. Vieira. ***Conversation Types***. Programming Languages and Systems, 18th European Symposium on Programming, ESOP 2009, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2009, York, UK, 2009. Springer-Verlag, Lecture Notes in Computer Science 5502, 2009.

11. Vasco T. Vasconcelos. ***Session types for linear multithreaded functional programming***. Proceedings of the 11th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming, PPDP 2009, Coimbra, Portugal, ACM, 2009.

12. Simon Gay and Vasco T. Vasconcelos and Antonio Ravara and Nils Gesbert and Alexandre Z. Caldeira. ***Modular Session Types for Distributed Object-Oriented Programming***. Proceedings of the 37th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2010, Manuel V. Hermenegildo, Jens Palsberg editors. Madrid, Spain, ACM, 2010.

13. Mário Pires and Luís Caires. ***A Type System for Access Control Views in Object-Oriented Languages***. Proceedings of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security, ARSPA-WITS 2009. Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2010, Springer-Verlag, Lecture Notes in Computer Science, 2010.

14. Ivan Lanese, Jorge A. Pérez, Davide Sangiorgi, Alan Schmitt: **On the Expressiveness of Polyadic and Synchronous Communication in Higher-Order Process Calculi**. Automata, Languages and Programming, 37th International Colloquium, ICALP 2010, Bordeaux, France, July 6-10, 2010, Proceedings, Part II. Lecture Notes in Computer Science 6199 Springer 2010: 442-453.

15. Hugo Aguiar and João Seco and Lúcio Ferrão. ***Profiling of Real World Web Applications***. Proceedings of the Workshop on Parallel and Distributed Systems: Testing, Analysis, and Debugging, Held as Part of the International Symposium on Software Testing and Analysis, ISSTA 2010, ACM, Trento, Italy, 2010.

16 . Filipe Militão and Luís Caires and Jonathan Aldrich. ***Aliasing control with view-based typestate***. Proceedings of the 11th International Workshop on Formal Techniques for Java-like Programs, Bart Jacobs and Frank Piessens, editors. Held as Part of the European Conference on Object Oriented Programming, ECOOP 2010, Maribor, Slovenia, ACM Library, 2010.

17. Vasco T. Vasconcelos, Francisco Martins, and Tiago Cogumbreiro. **Type inference for deadlock detection in a multithreaded typed assembly language**. In 3rd Programming Language Approaches to Concurrency and Communication-cEntric Software (PLACES), volume 17 of EPTCS, pages 95–109, 2010.

18. Luísa Lourenço and Luís Caires. ***Inference of Conversation Types for Distributed Multiparty Service Based Systems***, International Workshop on Programming Language Approaches to Concurrency and Communication-cEntric Software (PLACES), 2010.

19. Robert J. Simmons and Bernardo Toninho and Frank Pfenning. **Distributed deductive databases, declaratively**: **The L10 logic programming language**. ACM SIGPLAN 2011 X10 Workshop, 2010.

20. Francisco Martins, Vasco T. Vasconcelos, and Tiago Cogumbreiro. **Types for X10 Clocks**. In 4th Programming Language Approaches to Concurrency and Communication-cEntric Software (PLACES), volume 69 of EPTCS, 2010.

21. Robert J. Simmons and Bernardo Toninho. **Constructive Provability Logic**. Electronic Notes in Theoretical Computer Science, 2010.

22. Miguel Domingues, João Seco. **LiveWeb - Core Language for Web Applications**. INFORUM 2011, Actas do Symposium de Informática. Coimbra, Portugal, 2010.

23. Marco Giunti and Vasco T. Vasconcelos. **A linear account of session types in the pi calculus**. In 21st International Conference on Concurrency Theory (CONCUR), volume 6269 of LNCS, pages 432–446. Springer, 2010.

24. Luís Caires, Frank Pfenning: **Session Types as Intuitionistic Linear Propositions**. CONCUR 2010 - Concurrency Theory, 21th International Conference, CONCUR 2010, Paris, France, August 31-September 3, 2010. Proceedings. Lecture Notes in Computer Science 6269 Springer 2010.

25. Bernardo Toninho, Luís Caires: **A Spatial-Epistemic Logic for Reasoning about Security Protocols**. Proceedings 8th International Workshop on Security Issues in Concurrency SeCCO. EPTCS 51 2010.

26. Dimitris Mostrous and Vasco T. Vasconcelos. **Session typing for a featherweight Erlang**. In 11th International Conference on Coordination Models and Languages (Coordination), volume of 6721 LNCS, pages 95–109, Springer, 2011.

27. Luís Caires, Jorge A. Pérez, João Costa Seco, Hugo Torres Vieira, Lúcio Ferrão: **Type-Based Access Control in Data-Centric Systems**. Programming Languages and Systems - 20th European Symposium on Programming, ESOP 2011, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2011, Saarbrücken, Germany. Lecture Notes in Computer Science 6602 Springer 2011.

28. Mario Bravetti, Cinzia Di Giusto, Jorge A. Pérez, Gianluigi Zavattaro: **Adaptable Processes**. Formal Techniques for Distributed Systems - Joint 13th IFIP WG 6.1 International Conference, FMOODS 2011, and 31st IFIP WG 6.1 International Conference, FORTE 2011. Proceedings. Lecture Notes in Computer Science 6722 Springer 2011.

29. Luís Caires, Hugo T. Vieira: **Analysis of Service Oriented Software Systems with the Conversation Calculus**. Proceedings 7th International Workshop on Formal Aspects of Component Software, Lecture Notes in Computer Science 6921 Springer 2011.

30. Bernardo Toninho, Luís Caires, Frank Pfenning: **Dependent session types via intuitionistic linear type theory**. Proceedings of the 13th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming, July 20-22, 2011, Odense, Denmark. ACM 2011.

31. Luis Caires, Frank Pfenning and Bernardo Toninho. **Proof-Carrying Code in a Session-Typed Process Calculus**. Proceedings of the First International Conference on Certified Programs and Proofs CPP 11, Lecture Notes in Computer Science, Springer-Verlag, 2011.

32. Miguel Rebelo and Lúcio Ferrão. **Optimization of Web Applications Guided by Run-Time Usage Data**. INFORUM 2011, Actas do Symposium de Informática. Coimbra, Portugal, 2011.

33. Hugo López and Jorge A. Pérez. **Time and Exceptional Behavior in Multiparty Structured Interactions**. Post-proceedings of Web Services and Formal Methods - 8th International Workshop, WS-FM 2011, Lecture Notes in Computer Science, Springer-Verlag, 2011.

34*. Pedro Baltazar, Dimitris Mostrous, and Vasco T. Vasconcelos. **Linearly Refined Session Types**. In Linearity'12, volume 101 of EPTCS, pages 38-49, 2012.

35*. Luís Caires, Frank Pfenning, Bernardo Toninho: **Towards concurrent type theory**. TLDI 2012: 1-12. ACM.

36*. Henry DeYoung, Luís Caires, Frank Pfenning, Bernardo Toninho: **Cut Reduction in Linear Logic as Asynchronous Session-Typed Communication**. CSL 2012: 228-242. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik 2012 LIPIcs.

37*. Jorge A. Pérez, Luís Caires, Frank Pfenning, Bernardo Toninho: **Linear Logical Relations for Session-Based Concurrency**. ESOP 2012: 539-558. Springer-Verlag Lecture Notes in Computer Science

38*. Bernardo Toninho, Luís Caires, Frank Pfenning: **Functions as Session-Typed Processes**. FoSSaCS 2012: 346-360. Springer-Verlag Lecture Notes in Computer Science

39*. Pedro Baltazar, Luís Caires, Vasco T. Vasconcelos, and Hugo T. Vieira. **A Type System for Flexible Role Assignment in Multiparty Communicating Systems**. In *7th International Symposium on Trustworthy Global Computing*, 2012, Lecture Notes in Computer Science, Springer-Verlag.

Papers produced within the project, published after 31-12-12 (4)

40*. Luís Caires, João Costa Seco: **The type discipline of behavioral separation**. POPL 2013: 275-286. ACM.

41*. Luís Caires, Jorge A. Pérez, Frank Pfenning, Bernardo Toninho: **Behavioral Polymorphism and Parametricity in Session-Based Communication**. ESOP 2013: 330-349. Springer-Verlag Lecture Notes in Computer Science.

42*. Bernardo Toninho, Luís Caires, Frank Pfenning: **Higher-Order Processes, Functions, and Sessions: A Monadic Integration**. ESOP 2013: 350-369. Springer-Verlag Lecture Notes in Computer Science.

43*. Luísa Lourenço and Luís Caires. **Information Flow Analysis for Valued-Indexed Data Security Compartments**. In 8th International Symposium on Trustworthy Global Computing, 2013, Lecture Notes in Computer Science, Springer-Verlag.

9.5. Number of restricted reports (confidential documents)

7

9.6. List of restricted reports (confidential documents)

44. Luís Caíres, João Seco, Lúcio Ferrão, António Melo. **Flow Language Domain Specific Language preliminary specification**, 2009.

45. Luís Caíres, João Seco, Lúcio Ferrão, António Melo. **BPM Language Domain Specific Language preliminary specification**, 2009.

46. Luís Caíres, João Seco, Lúcio Ferrão, António Melo. **Module Language Domain Specifc Language preliminary specification**, 2010.

47. Luís Caíres, Gonçalo Borrega, Lúcio Ferrão, António Melo, João Seco. **OutSystems Application Model**, 2011.

48. Luís Caíres, Gonçalo Borrega, Lúcio Ferrão, António Melo, João Seco. **Role Based Security Model**, 2011.

49*. Lúcio Ferrão, António Melo, Hugo T. Vieira, João Seco, Gonçalo Borrega, David Nunes Luís Caíres. **Rich Query Editor Model**, 2012.

50*, Lúcio Ferrão, António Melo, Hugo T. Vieira, João Seco, Gonçalo Borrega, Luís Caíres. **Widget Abstraction Mechanisms Model**, 2012.

9.7. Number of Patents

1

9.8. List of Patents

(Restricted – US Patent pending**)**

51*. Gonçalo Borrega, Lúcio Ferrão, António Melo, Luís Caires, João Seco. **Pending U.S. Patent Application No. 13/418,922 "Systems, Methods, and Apparatus for Model-Based Security Control",** Docket No. OUT-006 (120398/210180), 2012**.**

9.9. Number of Ph.D. Thesis

2

9.10. Number of Master Thesis

10

9.11. List of Ph.D. and Master Thesis

52. Mário Pires, ***A Type System for Access Control in Object Oriented Languages***, Master Thesis FCTUNL, 2009.

53. Bernardo Toninho. ***A Tool and Logic for Local Reasoning About Security Protocols***, Master Thesis FCTUNL, 2009.

54. Jason Reed. ***A Hybrid Logical Framework***. PhD Thesis, Carnegie Mellon University, 2009.

55. Hélio Dolores. ***Optimizations in a Programming Language for Web Applications***, FCTUNL / OutSystems SA, 2009. Master Thesis. Supervisors: Lúcio Ferrão and Luís Caires.

56. Hugo Vieira. ***A Calculus for Modeling and Analyzing Conversations in Service-Oriented Computing***. PhD Thesis, FCT UNL, 2010.

57. Luísa Lourenço. ***Type Inference for Conversation Types***, Master Thesis FCTUNL, 2010.

58. Hugo Aguiar. ***Profiling of Web Applications in Production Environments***, Master Thesis FCTUNL / OutSystems SA, 2010. Supervisors: Lúcio Ferrão and João Costa Seco.

59. Miguel Rebelo. ***Profile guided adaptive optimizations in a DSL for Web Applications***, Master Thesis FCTUNL / OutSystems SA, 2011. Supervisors: Lúcio Ferrão and Luís Caires.

60*. Miguel Alves. ***Integrated Data model and DSL modifications***. Master Thesis FCTUNL / OutSystems SA, 2012. Supervisors: Lúcio Ferrão and João Costa Seco.

61*. Nuno Grade. ***Data queries over heterogeneous sources***, Master Thesis FCTUNL / OutSystems SA, 2012. Supervisors: Lúcio Ferrão and João Costa Seco.

62* André Simões. ***Expressiveness Improvements of OutSystems DSL Query Primitives***. Master Thesis FCTUNL / OutSystems SA, 2012. Supervisors: Hugo Lourenço and Hugo T. Vieira.

63* Paulo Ferreira. ***Information flow analysis for using data-dependent logical propositions***. Master Thesis FCTUNL 2012. Supervisors: Carla Ferreira and João Seco.

9.12. Number of Prototypes

4

9.13. List of Prototypes

64. João Seco, Miguel Domingues, Paulo Ferreira, Luísa Lourenço, Luis Caires. First version of the LIVEWeb Web verified programming system, FCTUNL, 2010.

65. João Seco, Miguel Domingues, Paulo Ferreira, Luísa Lourenço, Luis Caires. Second version of the LIVEWeb Web verified programming system, FCTUNL, 2011.

66. Lúcio Ferrão, Gonçalo Borrega, António Melo, João Seco, Luis Caires. Prototype of Role-based Model Driven Security for the OutSystems Service Studio, OutSystems SA, 2011.

67*. João Seco, Miguel Domingues, Paulo Ferreira, Luísa Lourenço, Luis Caires. Third version of the LIVEWeb Web verified programming system, FCTUNL, 2012.

9.14. Number of Talks, presentations and dissemination actions delivered

35

9.15. List of Talks, presentations and dissemination actions delivered

We do not include here the presentations of refereed conference papers listed above:

68. Luís Caires. ***Dynamic Control of Interference with Spatial-Behavioral Types***, **Principles of Programming** (PoP) Seminar, Carnegie Mellon Department of Computer Science, February 2009, Pittsburgh, USA.

69. Vasco Vasconcelos. ***The INTERFACES Project***, CMU|Portugal Research Projects Kick off, March 2009, FCT/MCTES, Lisboa, Portugal.

70. Luís Caires. ***On Session Types and Linear Logic (joint work with Frank Pfenning)***, **IFIP WG 2.2 Meeting**, September 2009, Bologna, Italy.

71. Frank Pfenning. ***The INTERFACES Project***, Panelist at the **Innovation Forum** on Security and Critical Infrastructure Protection (NET-SCIP), February 2010, Coimbra, Portugal.

72. João Costa Seco. ***Programming Language Techniques for Software Validation***, **OutSystems SA Engineering Kickoff** 2010 meeting at FCT/UNL, April 2010, Lisbon, Portugal.

73. Luís Caires. ***The INTERFACES Project***, **Innovation Forum** on Future Internet Services and Technologies (NET-FIT), February 2010, Lisbon, Portugal.

74. Vasco Vasconcelos. ***Modular Session Types for Distributed Object-Oriented Programming***, **ISR Seminar Series**, Carnegie Mellon Institute for Software Research, May 2010, Pittsburgh, USA.

75. João Costa Seco. ***Type Based Access Control to Database Entities*** (joint work with Luís Caires and Jorge Perez and Hugo T. Vieira), International Workshop on Relations and Data Integrity Constraints and Languages, RADICAL 2010, **Microsoft Research, Roger Needham Building**, May 2010, Cambridge, UK.

76. Luís Caires. ***The INTERFACES Project***, Dissemination Talk at the **UMIC Future Internet Technologies Forum**, May 2010, Lisboa, Portugal.

77. António Melo. ***The OutSystems view on FIT***, Dissemination Talk at the **UMIC Future Internet Technologies Forum**, May 2010, Lisboa, Portugal.

78. João Seco. **Language Based Security for Database Access Control**. NET-SCIP Workshop, Universidade do Porto, October 13, 2010, Porto, Portugal.

79. João Seco. Participation in ICT Portugal presentation at the Future Internet Conference Week organized by the UE, Ghent, December 2010, Belgium.

80. Frank Pfenning. **Dependent Session Types via Intuitionistic Linear Type Theory**. Behavioral Types Workshop: 19th-21st April 2011

81. Luis Caires. **On session types, linear logic, and observational equivalences**. Behavioral Types Workshop: 19th-21st April 2011.

82. Hugo Vieira. **Analyzing Multiparty Interaction using Conversation Types**. Behavioral Types Workshop: 19th-21st April 2011.

83. Vasco Vasconcelos. **Sessions, from types to programming languages**. Behavioral Types Workshop: 19th-21st April 2011.

84. Filipe Militão. **Aliasing control with view-based typestate**. Behavioral Types Workshop: 19th-21st April 2011.

85. Jonathan Aldrich, Luis Caires, Kohei Honda, James Leifer, Jakob Rehof. Panel: **Comparing approaches to behavioral types**. Behavioral Types Workshop: 19th-21st April 2011.

86. Hugo Vieira. **Modeling and Analyzing Conversations in Service-Oriented Computing. Departmental Seminar**, Charles University, Prague. 26th April 2011.

87. Antonio Melo. **INTERFACES and OutSystems: A Perspective on Academia-Industry Research Collaboration**. 2011 Annual Carnegie Mellon Portugal Program Conference, October 2011.

88. Lúcio Ferrão. **OutSystems Security Prototype Demo.** 2011 Annual Carnegie Mellon Portugal Program Conference, October 2011.

89. Frank Pfenning. **Certifying Distributed Software**. 2011 Annual Carnegie Mellon Portugal Program Conference, October 2011.

90. João Seco. **Validation of the Design and Architecture of Software Systems**, Seminar at Novabase SEG, November 2011.

91. João Seco. **Data Security in Web Apps based on Refinement Types**. Talk at Aeminium / INTERFACES workshop, November 2011.

92. Vasco Vasconcelos. **Checking Dynamic Roles in Multiparty Communication**. Talk at Aeminium / INTERFACES workshop, November 2011.

93. Luis Caires. **Interface Certification for Software Services**. Talk at Aeminium / INTERFACES workshop, November 2011.

94. António Melo. **Validation Issues in Web Application Development**. Talk at Aeminium / INTERFACES workshop, November 2011.

95*. Frank Pfenning. **Towards Concurrent Type Theory**, TLDI, Jan 2012.

96*. Luís Caires. **The Type Discipine of Behavioral Separation**. **Principles of Programming** (PoP) Seminar, Carnegie Mellon Department of Computer Science, May 2012.

97*. Bernardo Toninho. Speaking Skills Talk: **A Logical Foundation for Proof-Carrying Communicating Processes**, Carnegie Mellon Department of Computer Science, May 2012.

98*. Filipe Militão. Speaking Skills Talk: **Rely-Guarantee View Typestate**, Carnegie Mellon Department of Computer Science, May 2012.

99*. Jorge A. Perez. PPS Seminar, PPS Laboratory, Université Paris Diderot.Talk title: **Linear Logical Relations and Observational Equivalences for Session- Based Concurrency**, June 2012.

100*. Luís Caires. **The Type Discipine of Behavioral Separation**. **IFIP WG 2.2 Meeting**, Amsterdam, September 2012.

101*. Bernardo Toninho. **Linear Logic: A logical foundation for concurrent computation**, Choco Meeting, invited Seminar at Ecole Normal Superieure de Lyon, October 2012.

102*. Hugo T. Vieira. **2-way academia-industry knowledge transfer in the INTERFACES project**. **Panel Presentation.** CMU Portugal Program Symposium, January 2013.

9.16. Number of Press Releases

6

9.17. List of Press Releases

103. Semana Informática (24 June 2011)
Joint Venture Académica optimiza segurança do software
http://www.cmuportugal.org/uploadedFiles/news/news_2010/10-06-2011%20%20Joint%20Venture%20académica%20optimiza%20segurança%20de%20software%20%20Semana%20Informática.pdf

104. Computer World (31 May 2011)
OutSystems oferece aplicações para acelerar disponibilização
http://www.computerworld.com.pt/2011/05/31/outsystems-oferece-aplicacoes-para-acelerar-disponibilizacao/

105. CMU PT Web site (May 2010)
INTERFACES Project Responds to Security Concerns
http://www.cmuportugal.org/tiercontent.aspx?id=2710

106. Agile Software.ORG News (14 Out 2009)
Partnership promotes knowledge transfer between academic and corporate research
http://agile-software.org/news/outsystems-partners-with-universidade-nova-de-lisboa/

107. Quality Online (12 Out 2009)
OutSystems assina parceria com Universidade Nova de Lisboa
http://www.cmuportugal.org/uploadedFiles/news/ICTI_in_the_Portuguese_News,_2009/OutSystems%20assina%20parceria%20com%20Universidade%20Nova%20de%20Lisboa_qualidade%20online_12out09.docx.pdf

108. Diário de Notícias (10 Out 2009)
OutSystems e UNL estudam sistema de informação ágil
http://www.dn.pt/inicio/ciencia/interior.aspx?content_id=1386120&secc

9. Patents

Gonçalo Borrega, Lúcio Ferrão, António Melo, Luís Caires, João Seco. ***Pending U.S. Patent Application No. 13/418,922 "Systems, Methods, and Apparatus for Model-Based Security Control",*** *Docket No. OUT-006 (120398/210180), 2012.*

10. Prototypes & Testbeds

João Seco, Miguel Domingues, Paulo Ferreira, Luísa Lourenço, Luis Caires. ***First version of the LIVEWeb Web verified programming system****, FCTUNL, 2010.*

João Seco, Miguel Domingues, Paulo Ferreira, Luísa Lourenço, Luis Caires. ***Second version of the LIVEWeb Web verified programming system****, FCTUNL, 2011.*

Lúcio Ferrão, Gonçalo Borrega, António Melo, João Seco, Luis Caires. ***Prototype of Role-based Model Driven Security for the OutSystems Service Studio****, OutSystems SA, 2011.*

João Seco, Miguel Domingues, Paulo Ferreira, Luísa Lourenço, Luis Caires. ***Third version of the LIVEWeb Web verified programming system****, FCTUNL, 2012.*

11. Technology Transfer

Very fruitful bidirectional knowledge exchanges were developed and are still occurring between the academic partners and OutSystems SA, the industrial partner of INTERFACES. Such activities are leading to innovative solutions with practical impact, focused on the design of high tech software development and analysis tools.

An associated R&D partnership established between OutSystems and FCT UNL (in the context of the Flex-Agile project collaboration) during Y1 continued very actively during the whole project, initially motivated by the joint involvement in INTERFACES, and is still running as of June 2013.

OutSystems is a software company providing an industry leading All-in-One Agile Platform for rapid delivery and management of web business applications that are built for continuous change, and one of the few software development companies in Portugal that successfully acts in the global market. OutSystems core product is a fully-fledged software development environment for web applications, which extracts value from the integration of principled static analysis and program language-based techniques in their DSL, compiler, and runtime infrastructure. The OutSystems development environment provides the context in which many of INTERFACES outcomes will be validated, taking into account the requirements of real software web/internet development. Several concepts developed within our research teams will get eventually incorporated in products, as a consequence of our knowledge / technology transfer approach based on core-language development and prototyping.

Conversely, we find extremely valuable that OutSystems is providing us the academic partners with research challenges motivated by real needs of users, or by product improvement requirements (we thank Antonio Melo, Lúcio Ferrão, Gonçalo Borrêga, David

Nunes, and Rodrigo Coutinho for all their support and commitment to extract value to everyone from our collaborations). Some of these challenges are engineering oriented, while others have led to theoretical results. We give below some examples of our collaborative knowledge transfer activities, and of their results.

FCTUNL and OutSystems are holding routine work meetings (OutSystems SA headquarters, roughly thrice a month) - the Carnegie Mellon team (Pfenning) visited OutSystems for several occasions to discuss collaborations (see Interactions section below). Usually, around 5 people attended each meeting, and more than 8 different people from different areas of the company have participated (R&D, Product Management, Services). Covered themes in Y2 have included the development of a comprehensive declarative security model for the Agile Platform, a proposal for modularity, versioning, and "weak" module references, a proposal for an application definition and installation model, with sharing of modules, installation scripts, tutorials, and seed data, which helped the app store development effort (the OutSystems AppStore was launched at the OutSystems NextStep 2011 event), and preliminary discussions on runtime report generation.

Covered themes in Y3 have included the conclusion of a US patent submission [51] on the development of a comprehensive declarative security model for the Agile Platform, a model for declarative and validated edition of database queries [49], and a widget abstraction mechanism for extensible (graphical) user interfaces. This later development is an ongoing interesting effort leveraging programming language techniques in the domain of composition reusable modular verified user interfaces, in which usability concerns have played a major role [50]. These developments were related to the focus of OutSystems platform launched on NextStep 2013 event, which was usability and UX.

At major milestones, **reports** have been presented in formal sessions to the engineering team [44,45,46,47,48,49,50].

The collaboration with OutSystems lead to the following results we would like to summarize: a joint **paper at a top conference** [27], on static analysis of access control for database access operations, co-authored by UNL and Outsystems researchers, a **prototype integration** of this technique in the OutSystems service studio [66], a **US Patent** based on an application of this work [51], several Master thesis developed by students in Outsystems internships, on topics related to programming language design and implementation and web applications and very relevant for the INTERFACES project. Delivered MSc thesis co-supervised by FCTUNL and OutSystems researchers have delivered several improvements on the Outsystems compiler backend and frontend [55,58,59,60,61,62]. Some of them have led to other publications [15,27,32]. It is expected that some of these results will eventually get through the development pipeline of OutSystems. Outsystems and UNL are also involved in the **QREN** project on "**Long Tail Business Applications Platform**" where several themes motivated by the INTERFACES project (but not exclusively), will be pursued.

Other interactions are worth mentioning. The OutSystems SA Engineering Kickoff meeting 2010 took place at FCTUNL, and featured an invited keynote by INTERFACES researcher

Seco on "**Programming Language Techniques for Software Validation**". OutSystems SA researchers have also contributed occasionally with **talks at Master level courses** both at FCTUNL and FCUL, and participated in dissemination sessions to raise students awareness about practical software engineering and construction issues.

12. Industry Involvement

(Document written by the company involved in the project stating the achievements, challenges and outcomes)

13. INTERFACES Description and FAQ (aimed at the general public)

What is INTERFACES really about?

Who did never experienced a sudden crash of his computer, perhapsaccompanied by a mildly understandable error message? To make things worst, events of the kind may cause precious information to get definitively lost, and bring more or less serious consequences,depending on what is at stake: the last holiday photos, last year finance records, or the clinical history of so many patients. Malfunctions of these kind are only very rarely due to hardware or physical defects, but actually to programming mistakes (also known as "bugs"), which unfortunately are still rather frequent.

Modern software systems are complex and open to extension, so making sure that "programs don't go wrong" is far from a trivial challenge posed to software developers and service providers, in particular if security concerns enter into play (e.g., you must be sure that your Facebook private data is only accessed by authorized users, only you and your friends). Integrity and security concerns are critical for large scale software systems, with huge numbers users, changing every day, such as most web based applications running in the internet. Making sure that most parts of a huge software system is trustworthy is a formidable task even for the most experienced and skilled development teams. What if the correctness and safety of software could be enforced by automated means, so to help error prone human developers to avoid common pitfalls and bugs? Would it be possible to build programs capable to automatically analyze and possibly correct errors in software, saving costly human resources, even when such software is constructed from several pieces collected from the internet, and subject to strict security and resource usage requirements?

The INTERFACES project tackles these challenges by researching all the way from theoretical principles to systems development, leading to the development of automated tools that will improve companies and programmers ability to build safe and secure web software applications. A key novelty of this project is the use of sophisticated logic and type systems that will lead to the design of programs that can actually automatically analyze other programs, and help developers to detect and correct errors even before the modules are installed, just by looking to the way they

glue to each other, that is, to their INTERFACES.

What are the general goals of the project?

A broad objective of this partnership is the promotion of both-ways knowledge transfer between top notch academic research and industrialR&D, towards the development of innovative, agile, and trustworthy ways of producing Internets based software systems and applications.

The development of software applications is based on the use by teams of highly skilled software engineers of sophisticated tools called "programming languages" and "programming environments". Unfortunately, most existing programming languages and environments used by industry do not provide enough help for software engineers to avoid programming and design errors. In a collaboration between the Department of Computer Science at the Carnegie Mellon University, the CITI, FCT, Universidade Nova de Lisboa, LASIGE, FCUL, Universidade de Lisboa and the Portuguese multinational leading software company OutSystems SA, the project INTERFACES will develop new programming languages, techniques and tools that will warn software engineers when developing interned-based software systems that it may incur into some kinds of serious errors, even before it gets placed into operation. Our research will contribute not only for reducing development and maintenance costs, but the also to increase the quality of products and services delivered to the end users.

INTERFACES results are very general, and may be applied in many different useful practical situations. This is a consequence of the technical approaches followed in the project, where we will be delivering not a specific application or system, but actually computer programs that may automatically check other computer programs for correctness and compliance to security and integrity. This requires the use of sophisticated mathematical program analysis methods, using logics and types, and their implementation in programs that may perform this reasoning tasks by themselves without human intervention.

In what concrete situations will INTERFACES research objectives be useful?

It is easy to provide examples of situations where INTERFACES results will be extremely useful. In a fast changing world, web applications are subject to just too frequent changes in their requirements. Changes are needed because, say, the business processes need to be modified for management reasons, to save resources, because the rules of the business or the legislation changed, or just because new features need to be added, to keep competitiveness. Typically, changing the functionality of a large software system while it runs, without disturbing the information stored in its large databases, the security rights of its users, and preserving everything which is already stable and working well, is a challenging task. By proposing new sophisticated interface languages at the level of software building blocks, INTERFACES will make sure that the system will continue to operate in a safe and secure way.

For example, suppose that a web services company wants to add a selective information sharing facility to a cloud application, to allow the users to autonomously make public some of private information (for example, bank account number, or a password for another service) but only to some other selected colleagues. This is a critical functionality that if erroneously implemented by the software developer will affect the information privacy of large numbers of users. How to make sure that the software piece that implements the new selective publication mechanism is indeed secure, and only authorized peers will indeed be able to see the private information? In a scenario such as this, INTERFACES will be able to automatically analyze the developed code and signal (for example, painting the code red on the programmer screen) what parts are insecure. In some

situations, it will be even possible for INTERFACES to automatically correct or adapt the software, so that it may comply with the intended integrity requirements.

In what stage is currently the project?

INTERFACES is now approaching the end of the first year. We have already obtained several interesting results, namely techniques to make sure that participants in distributed business processes interchange messages according to previously agreed protocols, and their incorporation in software verification tools, and new ways to combine software pieces in a running system, while making sure that integrity properties are preserved. Several of these technical results have been published or are currently submitted to international conferences and journals. We are also working on a prototype of a self-correcting web-application development system, able to detect possible security breaches before they happen, and warn the software developer at the right time.

Why is it important for INTERFACES to be developed within CMU|Portugal?

The CMU-Portugal initiative offers a unique opportunity to bring together leading research teams in the areas of programming languages, logical frameworks, logics for security and resources, fields where CMU is worldwide known by its contributions, and types, logics, and runtime systems for concurrent, distributed and service-oriented systems, to explore relationships and synergies. An important characteristic of INTERFACES is that it moves towards bridging basic research results to validation and product improvement in real systems, in collaboration with the industrial partner OutSystems.

What is the importance of the collaboration with OutSystems?

OutSystems is a Portuguese multinational software company providing an industry leading All-in-One Agile Platform for rapid delivery and management of web business applications that are built for continuous change (see more information at http://www.outsystems.com/agile/). Outsystems accumulated experience in the design of programming environments for the agile development of web based information system, together with the experience of the academic partners in programming language research is fostering a bidirectional knowledge transfer with the potential of generating results of high technological and scientific impact.