RELEASE - RELiablE And SEcure computation Group

Paul Crocker, João Paulo Fernandes, Simão Melo de Sousa

DIUBI/LISP

2017

Scientific Goals

Design of Modern, Reliable and Secure Computer/Information Systems

- Concepts and Methodologies,
- Tools, programming languages and software development environments
- Applications
- Technology Transfer

Strategic Goals

- Technology transfer from our FM & Security expertise to computer and software industry
- Creation of a recognized competence center in computer/information system reliability and security.
- Foster security and formal methods research and applications

Research Area

Better practice comes from good theories. *(Kurt Lewin)*

João Paulo: Science and Technologies for Software Engineering
Paul: Security/Cryptography, Distributed Systems, Operating Systems
Simão: I'm a programmer!

- **Computer Systems Reliability**: Formal Methods, Formal Specification and Verification of programs, Software Development, Software Testing, Validation and Verification.
- **Computer Systems Security**: Mobile Code Security, Smart Cards/Portable Cryptographic Devices, Applied Cryptography, Security in Ubiquitous Computing/Cloud Environment.
- **Computer Aided Reasoning**: Automatic Demonstration, Proof Assistants, Computational Logic, Application to Computer Science.
- **Programming Languages Design**: Type Systems, Operational Semantics, Functional Programming, Static Program Analysis, Program Transformation.

Funded Research Projects

- ICT COST Action IC1306 Cryptography for Secure Digital Interaction
- ICT COST Action CA15123 The European research network on types for programming and verification (EUTYPES)

- ICT COST Action IC1202 - TACLe - Timing Analysis on Code-Level
- (FCT) Favas - 2010 - 2013
  A Formal Verification Platform for Realtime Systems
- (FCT) Cante - 2011-2013
  Descriptional and Computational Complexity of Formal Languages
- (FCT) Aviacc - 2012-2014
  Analysis and Verification of Critical Concurrent Programs
- (FCT) Rescue, 2008-2011
  REliable and Safe Code execUtion for Embedded systems.

Technology Transfer based and R&D Projects

- Stork (Multicert) - European Electronic Citizen Card
- Evolve (Critical Software - UM) - Evolutionary Verification, Validation and Certification.
- Prosinal (Efacec) - (SIL4) Certified Railway Signalling Systems.
- PROVA (Educed, Critical Software, UM) - Requirement Engineering Made Better
- PRICE (PT Inovação) - Privacy, Reliability and Integrity in Cloud Environments.
- SOFTSIM (PT Inovação) - Software based SIM cards.
- Automatic U/A Testing (PT Inovação)
- QuiVVER - centro de competência em qualidade, validação e verificação de software (CENTRO-07-CT62-FEDER-005009)
- Testing and Runtime monitoring for RTEMS (Edisoft)

A glimpse of our foundational work

Deductive Program Verification framework for assembly Programs

- Transformation techniques for ARM programs (From ARM to Why3ML via CFG transformations)
- Why3 powered platform for the formal verification of ARM programs
- Collaboration: Jean-Christophe Filliâtre (PROVAL - LRI/CNRS/INRIA)

Operational Semantics for the full Concurrent Separation Logic

- Definition and correctness proof
- Proof System and static analysers for concurrent programs
- Application to *safe-by-construction* lock-free concurrent programming

Abstraction carrying code framework for WCET analysis

- The issue: automatic adaptability and updates for realtime systems
  - Architectural Design: Proof Carrying Code
  - Abstract Interpretation based WCET Certificates (evidences of safety – may be hard to compute but are easy to check)
- Extension to multicore environment
- Collaboration: R. Whilhelm (U. Saarland - DE, & AbsInt)

(re)lease
RELiabIE And SEcure Computation Group

PROSINAL

- Goal : CENELEC SIL4 Railway Signaling System for the *Metro do Porto* - linha Aeroporto Sá Carneiro.
- Challenge: Software layer design , validation and certification (SIL4 - the highest) using Formal Methods in a very restrictive normative context (CENELEC). The first of its nature, to the best of our knowledge.
- Other Mission: set-up and training of a (formal) Validation team in an industrial context.
- Extension of the Scade toolset to deal with Function Block based HW.
  - a (pencil and paper proved) translation methodology and
  - a (HW level) testing framework with tests generated from SCADE models – allow for a better confidence on the translation process

(Highlight: First Signaling System **in the world!** formally and completely proved from scratch that reaches the new CENELEC SIL4 certification)

Price: Security in the Cloud

Project PRICE - Privacy, Reliability and Integrity in Cloud computing Environment

- Goals: Explore new support mechanisms for security in Cloud Systems
  - Authentication in Cloud Systems
    - ★ Set of Web Services Via Cartão do Cidadão (CC) Based Authentication
    - ★ Group Based Authentication
    - ★ Threshold Cryptography based on PKI and Digital Certificates
  - Encryption
    - ★ Identity Based Cryptography Scheme Based on CC
    - ★ Sticky Policies
    - ★ Security Policies bound to data and identity
    - ★ Homomorphic encryption
- Collaboration: PT-Inovação

PROVA: Engineering Made Better - From Requirements to Tests

- Motivation:
  - Requirements engineering processes are essentially manual and heavily based on text documentation, thus error prone and tedious.
  - As a consequence: traceability matrix and tests planning inherits from the requirement status.
  - both miss the automation opportunity
- Goals: provide, via an unifying computation platform, computational support for:
  - Requirement identification, categorization, elicitation, validation and recording
  - Automatic (system, integration and unit) Test Specification and generation according to the Requirement Specification.
- Several grants are available at Master level and/or for final year projects
- Collaboration: UM, Critical Software, Educed

QuiVVer Competence Center - Quality Validation and Verification of Software

- Our technology transfer platform
- Applied R& D targeted to our industrial partner's challenges/needs

A (non-extensive) perspective on the center facilities

State-of-the-art, multi platform processing devices...

- mobile devices;
- tablets;
- laptops, computers;
- high performance computing servers;
- embedded devices;
- software testing platforms (e.g. HP Quality Center, HP Sprinter);
- (in-house) cloud based solutions (testing as a service): **Niburu**.

A (non-extensive) perspective on the center facilities

... implemented in a state-of-the-art secure communication environment...

- video conference equipment;
- interactive boards;
- state of the art equipment for distance collaborative team work;
- secure storage facilities;
- highly efficient and configurable network equipment (VPN, privacy and confidentiality enforcement mechanisms, backup, data/network isolation).

A (non-extensive) perspective on the center facilities

- ISVV
- ability to design or co-design specific validation and verification methodologies and related tools support adapted to the partner's needs;
- ability to train validation and verification specialists;
- and academic evolving context (LISP) provides already trained young specialists.

Thank You!