SCIENCESPRINGDAY

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

DEPARTAMENTO DE INFORMÁTICA

Dependent Session Types

Bernardo Toninho

PhD Student

Co-advised by Frank Pfenning (CMU) and Luis Caires (FCT-UNL). Research focus on the logical foundations of concurrency.

SOFTWARE SYSTEMS / PLASTIC Team

CENTER FOR INFORMATICS AND INFORMATION TECHNOLOGIES

Objectives

We aim to enable the development of safe and secure applications by developing rigorous techniques that allow for the specification of rich interface contracts between communicating parties:

- Distributed web services are pervasive, but difficult to build in a safe and secure way.
- Traditional type systems for concurrency only specify very simple I/O behavior:
  Eg: Send a number and receive back a string of characters.
- No clear way of specifying properties of exchanged data:
  Eg: Send a buy request and get charged the correct amount.
- No sophisticated properties of the services themselves:
  Eg: Trusted service **A** is equivalent to service **B**.

Methodology

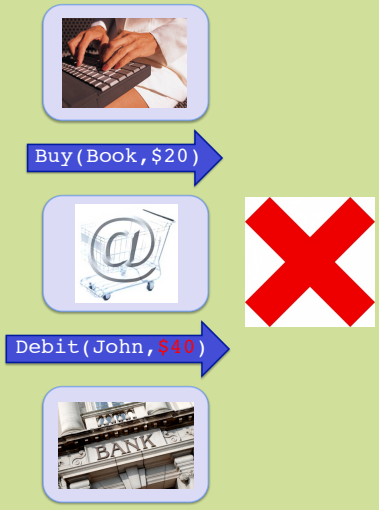
We develop a radical new approach to type theories for concurrency, based on an interpretation of logic as a language for describing concurrent systems:

- Investigate techniques to automatically ensure safe composition of web services.
- Integration of I/O behavior with sophisticated data properties.
- Precise account of digital certification of desired properties (i.e. self-certifying distributed services).
- Types as a rich interface description language, automatically verifiable **before** execution of the system.

Expected Results

- A type theory allowing the specification and certification of rich properties of distributed agents and their data:
  Eg: "An eShop cannot overcharge its clients";
  "Different providers of the shop service are equivalently safe";
- Natural extensions to handle varying degrees of trust and digitally signed proof certificates (i.e. ask for **proofs,** or trust the service).
- A unified language framework for distributed agents (programs), properties (types) and digital certificates (proofs).
- Multiple publications in top conferences of the field (PPDP'11, TLDI'12, ESOP'12, FoSSaCS'12, 2x ESOP'13).

$\text{buy} \multimap \text{receipt} \otimes 1$



$\forall b : \text{prod}.\forall c : \text{nat}.$
$\text{buy}(b, c) \multimap \text{receipt}(b, c) \otimes 1$

Funding:
FCT
INTER FACES
Information and Communication Technologies Institute
Carnegie Mellon | PORTUGAL
AN INTERNATIONAL PARTNERSHIP
FACULDADE DE