Language Based Security for Database Access Control

João Costa Seco Jorge A. Perez Hugo T. Vieira Luís Caires

CITI - FCT Universidade Nova de Lisboa
Certified Interfaces Project (with
Frank Pfenning CMU, Vasco Vasconcelos LASIGE, and Lúcio Ferrão OutSystems SA)

Security in software systems may be compromised when applications accidentally allow access to private data, which is typically due to programming mistakes. Such scenarios, where security follows from program correctness, arise naturally in the setting of business data-centric (web) applications which are currently of particular relevance. Such security issues may be addressed by Language Based Security [4, 5], which consists in using programming language related mechanisms to tackle security problems in software systems. The purpose of Language Based Security is to take advantage of the semantic leverage that language abstraction provides, and produce tools that ensure security properties by construction. These tools range from certifying compilers, to type systems that rule-out insecure programs.

Our research approach, in the PLASTIC research team[1], from the Software Principles and Methods area at CITI, is based on the development of new programming languages, logics and tools to model and statically verify properties of systems, many times focusing on security properties. Relevant research includes, for instance, the use of logics to reason about security properties of protocols in distributed systems [6], and the design of programming languages equipped with authorization primitives [3]. In the latter, access to object references is restricted by default, and permission to call methods on objects can only be obtained by means of runtime checking of certificates. The type system ensures, at compile time, that security policies are followed and that methods are not called without proper authorization.

In this talk, as a case study, we present a new research direction emerging from the Certified Interfaces research project[2], that aims at statically ensuring the confidentiality and integrity of data in programs, by means of logic and type-based techniques [1]. In particular, we tackle the problem of specifying and statically verifying access control policies that actually depend on data stored in databases. We build on the notion of refinement types [2], which combines standard type-theories with first order logic, to reason about access control to data stored in the database.

In our type system we may express properties like "a user can only see its own private photos" and ensure that a well-typed application always enforces the necessary verifications, for instance, by checking the session data for appropriate user credentials. In this work, we define a programming language that allows for access control policies to be defined in a declarative way and enforced by the software development environment. These techniques are available in a prototype implementation and are expected to be usable in real world tools such as the OutSystems SDE.

[1] Luís Caires, Jorge A. Perez, João C. Seco, and Hugo T. Vieira. Refinement Types for Database Access Control. Technical Report UNL-DI-3-2010.

[2] Tim Freeman and Frank Pfenning. Refinement Types for ML. In *PLDI*, pages 268–277, 1991.

[3] Mário Pires and Luís Caires. A Type System for Access Control Views in Object-Oriented Languages. In *ARSPA-WITS*, 2010.

[4] A Sabelfeld and A Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communication*, (21), 2003.

[5] F Schneider, G Morrisett, and R Harper. A language-based approach to security. In *Informatics – 10 years back. 10 years ahead*, number 2000, pages 86–101. Springer-Verlag, 2001.

[6] Bernardo Toninho and Luís Caires. A Spatial-Epistemic Logic for Reasoning about Security Protocols. In *8th International Workshop on Security Issues in Concurrency (SecCo'10)*, 2010.

[1] Programming LAnguageS for CommunicaTIon-Centric Software Systems at CITI, FCTUNL. L. Caires (PI), João Costa Seco, Carla Ferreira, António Ravara, Hugo Torres Vieira. `http://ctp.di.fct.unl.pt/PLASTIC`

[2] Certified Interfaces, NGN44-CMUPortugal, `http://ctp.di.fct.unl.pt/INTERFACES`