Results from the application of Algebraic Specification Techniques on DRM systems

Nikolaos Triantafyllou, Petros Stefaneas and Panayiotis Frangos

National Technical University of Athens

July 15, 2013

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION & RELIGIOUS AFFAIRS
MANAGING AUTHORITY

NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND

Co-financed by Greece and the European Union

Road Map

- Introduction
  - DRM - Mobile DRM
  - Problems of DRM Systems
- Using Algebraic Specifications for DRM
- Implementation: Cafe2JML

Digital Rights Management Systems (DRM)

- Control all aspects of the life cycle of consumption
- More than cryptographic techniques
- Licenses controlling under when an action on a content is authorized
- Open Mobile Alliance

OMA DRM System

- OMA REL
- OMA DRM
- OMA Rights Object Evaluation Algorithm

OMA DRM Problems

- Lack of formal Semantics
- Rights Object Evaluation Algorithm bug

Using Algebraic Specifications for DRM

- Lack of formal Semantics
- Triantafyllou, N., Ouranos, I., Stefaneas, P.S.,: Algebraic Specifications for OMA REL Licenses (IEEE International Conference on Wireless and Mobile Computing, Networking and Communications)
  - definition of OMA REL semantics
  - specification in CafeOBJ
  - Using rewriting logic; reason about the behavior of OMA REL licenses

Using Algebraic Specifications for DRM

- Rights Object Evaluation Algorithm causes the loss of execution rights
- not as easy as it seems (NP-complete problem)
- idea:
  - move the extra cost on the creation of licenses (Order Sorted Algebra)
  - use the Rights Object Evaluation Algorithm as the core to reduce implementation cost

Using Algebraic Specifications for DRM

- To use the Rights Object Evaluation Algorithm
- some safety properties had to be verified
- Triantafyllou, N., Ouranos, I., Stefaneas, P. S., Frangos P.: Formal Specification and Verification of the OMA License Choice Algorithm in the OTS/CafeOBJ Method (The International Joint Conference on e-Business and Telecommunications)

Using Algebraic Specifications for DRM

- Triantafyllou, N., Stefaneas, P. S., Frangos, P.: An Algorithm for Allocating User Requests to Licenses in the OMA DRM System (IEICE TRANSACTIONS on Information and Systems).
- new algorithm for the allocation of rights
- formally specified in CafeOBJ and verified that it does not cause a loss of rights

Using Algebraic Specifications for DRM

- How can one verify that the implementation will respect the specification???
- OTS/CafeOBJ very strong for verification of design
  - high abstraction level
  - support for specification and proof composition
  - object-orientated approach to specification
  - computer human interactive verification
- However no formal connection between specification and implementation!

Using Algebraic Specifications for DRM

- Design by Contract: Approach to designing software
  - formal, precise and verifiable interface specifications for software components
  - using contracts which are added to methods (Hoare Logic)
- recently renewed interest in DbC languages

Using Algebraic Specifications for DRM

- Open Java Modeling Language (openJML), DbC language for Java
- Open Source
- Supported/implemented by a big community, many institutions.

Using Algebraic Specifications for DRM

- variety of tools:
  - Runtime Assertion Checking (RAC)
  - Unit test, generation (JML/JUNIT)
  - Extensive Static Checking (ESC)
  - Verification tools

Cafe2JML

- Cafe2JML: Translation from OTS/CafeOBJ Specification to JML specification
- software development methodology:
  - Design verified by CafeOBJ
  - Compliance of implementation verified by openJML

Cafe2JML

- why not just CafeOBJ:
  - no guarantee that the implementation will respect the specification
- why not just JML:
  - can only reason about Java programs
  - can only reason that the implementation respects the specification, not about the properties of the specification
- why not just Cafe2Java:
  - due to the abstraction level of CafeOBJ not possible to automatically generate Java code

Cafe2JML

- currently conducting case studies
- Future work:
  - build a tool to automate the translation
  - formally prove the correctness of the translation

Thank you!!
Questions??