Karlsruher Institut für Technologie

Software Design and Quality

Verification of Access Control in Software Systems

Proposal
Julian Hinrichs

SOFTWARE-ENTWURF UND -QUALITÄT
INSTITUT FÜR PROGRAMMSTRUKTUREN UND DATENORGANISATION, FAKULTÄT FÜR INFORMATIK

Motivation

- Security-audit on an architectural level.
- Support of an soliticious software architect
- Recognize security flaws in the early stage of the development process

Foundations

- CoCoME
  - Hybrid Cloud Based Variant
  - Addition of the PickUp-Shop
- PCM
  - Component Developer
  - System Architect
- Role based Access Control

State of the Art

- PCM missing elements
  - Data processing
  - Analysis techniques
- UMLSec
  - Extend the differen tmodel elements to security relevant information
- SecureUML
  - Adding additional model elements to an UML element

Related Work

- Stephan Seifermann. “Architectural Data Flow Analysis”. In: 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016, Venice, Italy, April 5-8, 2016. 2016, pp. 270–271. doi: 10.1109/WICSA.2016.49 . url: https://doi.org/10.1109/WICSA.2016.49 .

Approach

- Defining Preconditions
  - Analysis goals
  - Access control matrix
  - Extend models with data flows

Approach

- Defining Preconditions
  - Analysis goals
  - Access control matrix
  - Extend models with data
- Transformation to a contraint system

Approach

- Defining Preconditions
  - Analysis goals
  - Access control matrix
  - Extend models with data
- Transformation to a constraint system
- Solve the constraint system

Approach

- Defining Preconditions
  - Analysis goals
  - Access control matrix
  - Extend models with data
- Transformation to a constraint system
- Solve the constraint system
- Transformation back to the model

Contributions

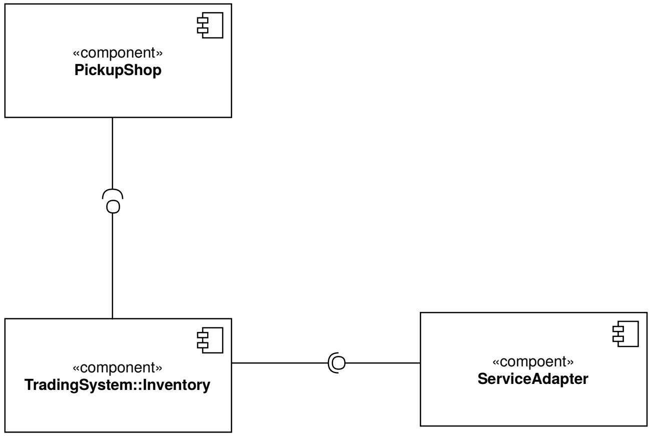
- Constraint solver
- Transformation to the constraint solver
- Transformation back to the model
- Extend PCM on a meta level
- Extend CoCoME models

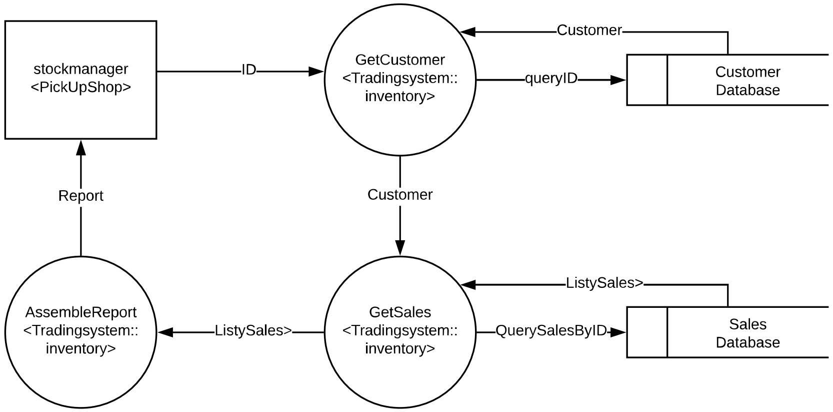
Evaluation

- Characteristic
  - Applicability
  - Comprehensiability
- Applied to CoCoME
  - Applicalibilty: Model and constraint solving
  - Comprehensiability: transformation back to the model

Evaluation

- Applicability
  - Extension of the PCM language
  - Extension of the CoCoME models
  - Transformation to the constraint system

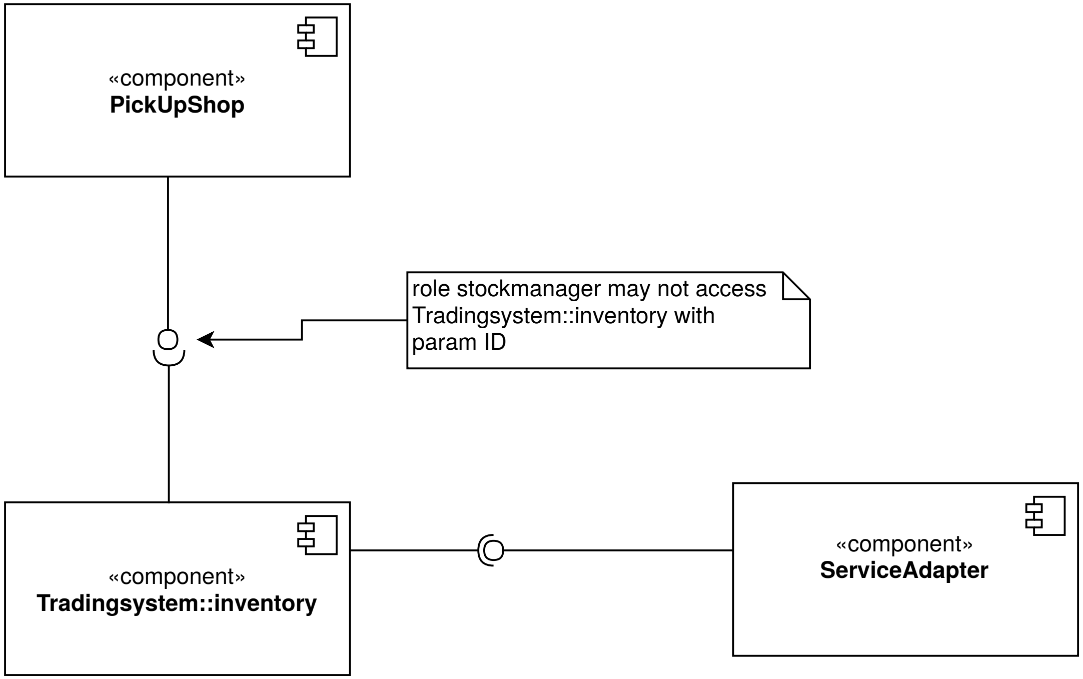




stockmanager <PickUpShop>
ID
GetCustomer <Tradingsystem:: inventory>
Customer
queryID
Customer Database
Report
Customer
AssembleReport <Tradingsystem:: inventory>
ListySales>
GetSales <Tradingsystem:: inventory>
ListySales>
QuerySalesByID
Sales Database

Evaluation

- Comprehensibility
  - Transformation back to the model



Organizational

- Schedule

Scenario 1	Preconditions, models, solver, evaluation	4 weeks
Scenario 2	Preconditions, models, solver, evaluation	4 weeks
Scenario 3	Preconditions, models, solver, evaluation	4 weeks
Puffer	Problems, corrections	2 weeks / 2 weeks

Organizational

- Riskmanagement
  - Extension of PCM
  - Development of constraint solver
  - Extension of CoCoME models
  - Transformation into a constraint system
  - Transformation back to the model