Improving Enterprise Architectures by Enforcing Business Process Access Control Requirements – Documentation of Evaluation

Roman Pilipchuk[1], Stephan Seifermann[2], Robert Heinrich[2], and Ralf Reussner[2]

[1] FZI Research Center for Information Technology, Germany
pilipchuk@fzi.de
[2] Karlsruhe Institute of Technology, Germany
{stephan.seifermann,robert.heinrich,ralf.reussner}@kit.edu

Abstract. This report documents the evaluation of our paper [2] that has been submitted to ECSA. We explain the structure of our data set [1] as well as the evaluation results. The documentation is not yet complete with respect to replicability instructions. However, it will be for the final submission.

1 Introduction

This reports gives an overview on the evaluation of our paper [2] that has been submitted to ECSA. Especially, it describes the contents of the corresponding data set [1] in Section 2 and gives insights in the classification of the evaluation results in Section 3. This first, preliminary version does not contain all information about setting up the environment to replicate the results of the automated steps yet. We will extend this documentation by detailed setup instructions after the paper has been accepted. We cannot provide this information before the deadline in the required degree of detail because of time restrictions.

The evaluation distinguishes the accuracy of the access control requirement (ACR) extraction and the accuracy of the architectural analysis. We evaluate the accuracy based on a case study. The studied case describes business processes of a German national art gallery. The case is the result of a consulting project for this art gallery. Therefore, the models are given in German. We translated all relevant parts in our publication [2] but the original models are still German. In this report, we stick to the German names in order to allow identifying entities in the corresponding models. Even if knowing the meaning of modeled elements would help in understanding the studied case in an intuitive way, it is not necessary.

2 Contents of Data Set

Our data set contains all code, models and results required to replicate the evaluation. An overview on the directory and file structure of the data set is given in the following:

```
/
├── code
│   ├── IntBIIS_LP
│   ├── Palladio-Addons-DataFlowConfidentiality
│   ├── Palladio-Supporting-DataFlowDiagram
│   ├── Palladio-Supporting-DataFlowDiagramConfidentiality
│   └── PallBPMNRMELaunchPlugin
├── models
│   └── ArtGallery
└── results
    ├── ACR
    │   ├── RoleModel.html
    │   └── TraceabilityModel.html
    └── dataTypeUsage.json
```

The `code` folder contains the source code of all automated steps of our approach. All artifacts are Eclipse projects ready to be imported. A full list of dependencies will be given in the final version of this report. The ACR extraction process requires metamodels located in `IntBIIS_LP` and the extraction algorithm located in `PallBPMNRMELaunchPlugin`. The architectural analysis requires the metamodel extensions for the Palladio Component Model (PCM) and the mapping to a data flow diagram as defined in `Palladio-Addons-DataFlow-Confidentiality`. The data flow diagram and the generic analysis logic is given in `Palladio-Supporting-DataFlowDiagram` and `Palladio-Supporting-Data-FlowDiagramConfidentiality`.

The `moderls` folder contains the PCM models of our studied case. The national art gallery case study is located in `ArtGallery`. The models can be opened in Eclipse if the Eclipse addons located in the `code` folder have been installed.

The `results` folder contains the results of the two steps of our evaluation for the national art gallery case study. The results of the ACR extraction step are located in the `ACR` folder. With respect to the evaluation, the role model `RoleModel.html` and the trace model `TraceabilityModel.html` are relevant. The results of the architectural data type usage analysis are located in `dataTypeUsage.json`.

3 Explanation of Evaluation Results

The following sections give some details on the answers of the two evaluation questions. Especially, it covers the classification step of the raw results.

3.1 Q1 What is the accuracy of the ACR extraction?

The 51 extracted ACRs can be found in the trace model of the `results/ACR/TraceabilityModel.html` file. Overall, the HTML contains 75 unique rows representing the activities of the ten business processes of the case study. Unique rows that have an entry in the column *BusinessPermission* indicate an ACR.

ACRs are then the projection of the column *role* and *BusinessPermission* where *BusinessPermission* is not empty. All things considered, there are 51 ACRs extracted by AcsALign that correspond with the amount and content of ACRs in the business processes in `models/ArtGallery`.

3.2 Q2 What is the accuracy of the architectural analysis?

MT1 Wrong data type produced in SEFF :

- Logical and Design Mistake: falsely defined parameters or return types of operation signatures
- **Service call:** Bestätigung des Leihgesuchs speichern
  - **Access control permissions ($D_{allowed}$):** WRITE Bestätigung des Leihgesuchs
  - **Data flow:** WRITE Bestätigung des Leihgesuchs, READ Leihgesuch
- **Architecture compliance analysis:**
  - **WRITE Bestätigung des Leihgesuchs:** In $D_{allowed}$ → allowed
  - **READ Leihgesuch:** Not in $D_{allowed}$ → forbidden
- Traceability information:
  - Business process: Negotiate Lending Conditions
  - Role: Vorstand: Direktor
  - Actor step: Antwort erhalten
  - Access control permissions: WRITE Bestätigung des Leihgesuchs

MT2 Wrong call in SEFF:

- Logical and Design Mistake: Logical and Design Mistake: falsely wired interfaces and operations of service effect specifications
- **Service call:** Hole fremdes Ausstellungkonzeptobjekt
  - **Access control permissions ($D_{allowed}$):** READ Fremdes Ausstellungsobjekt, WRITE Leihgesuch
  - **Data flow:** READ Ausstellungskonzeptobjekt für eigenes Werk
- **Architecture compliance analysis:**
  - **READ Ausstellungskonzeptobjekt für eigenes Werk:** Not in D_{known} → allowed
    - **READ Ausstellungsobjekt:** Not in $D_{allowed}$ → forbidden
    - **READ Restaurative Maßnahmen erforderlich:** Not in D_{known} → allowed
- Traceability information:
  - Business process: Negotiate Lending Conditions
  - Role: Sammlung und Wissenschaft: Kurator
  - Actor step: individuelles Leihgesuch schreiben
  - Access control permissions: READ Fremdes Ausstellungsobjekt, WRITE Leihgesuch

MT3 Wrong wiring of systems/components:

- Logical and Design Mistake: falsely wired systems and components
- **Service call:** Ausstellungsobjekt holen
  - **Access control permissions ($D_{allowed}$):** READ Ausstellungsobjekte (Coll.)
  - **Data flow:** READ Ausstellungobjekt, READ Fremdes Ausstellungsobjekt
- **Architecture compliance analysis:**
  - **READ Ausstellungobjekt:** Not in $D_{allowed}$ → forbidden
  - **READ Fremdes Ausstellungsobjekt:** Not in $D_{allowed}$ → forbidden
- Traceability information:
  - Business process: Negotiate Borrowing Conditions
  - Role: Sammlung und Wissenschaft: Kurator
  - Actor step: mündlich Leihanfrage entgegennehmen
  - Access control permissions: READ Bestätigung des Leihgesuchs, READ Ausstellungskonzept, WRITE Leihvertrag, WRITE Leihvertrag

MT4 Wrong data type refinement:

- Logical and Design Mistake: falsely built composite and collection data types
- **Service call: Leihvertrag erstellen**
  - **Access control permissions ($D_{allowed}$):** READ Bestätigung des Leihgesuchs, READ Ausstellungskonzept, WRITE Leihvertrag, WRITE CRM-Eintrag
  - **Data flow:** WRITE Leihvertrag
- **Architecture compliance analysis:**
  - **WRITE Leihvertrag:** In $D_{allowed}$ → allowed
    - **WRITE CRM-Eintrag:** In $D_{allowed}$ → allowed
    - **WRITE Ausstellungsobjekt:** Not in $D_{allowed}$ → forbidden
    - **WRITE Ausstellungsname:** Not in D_{known} → allowed
    - **WRITE Zeitraum:** Not in D_{known} → allowed
    - **WRITE Versicherungswert:** Not in D_{known} → allowed
    - **WRITE Fotoerlaubnis:** Not in D_{known} → allowed
- Traceability information:
  - Business process: Negotiate Lending Conditions
  - Role: Sammlung und Wissenschaft: Registrar
  - Actor step: Leihvertrag verhandeln
  - Access control permissions: READ Bestätigung des Leihgesuchs, READ Ausstellungskonzept, WRITE Leihvertrag, WRITE Leihvertrag

References

1. Pilipchuk, R., Seifermann, S., Heinrich, R., Reussner, R.: Evaluation data set. https://bit.ly/364z4a5 (2020)
2. Pilipchuk, R., Seifermann, S., Heinrich, R., Reussner, R.: Improving enterprise architectures by enforcing business process access control requirements. In: Software Architecture - 14th European Conference, ECSA 2020, L'Aquila, Italy, September 14-18, 2020, Proceedings. Lecture Notes in Computer Science, vol. tbd, p. tbd. Springer (2020), submitted