

# Refaktorisierung einer Architekturanalyse für Vertraulichkeit

**Praktikum Ingenieurgemäße Softwareentwicklung**

Alina Valta | 10. März 2022

# Inhaltsverzeichnis

## 1. Vertraulichkeitsanaylse

## 2. Modell

## 3. PCM2Prolog

## 4. Evaluierung

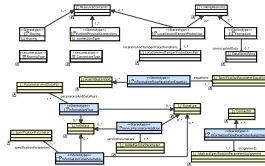
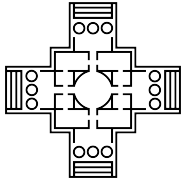
Vertraulichkeitsanaylse  
oooo

Modell  
ooooo

PCM2Prolog  
oo

Evaluierung  
o

# Vertraulichkeitsanalyse



```

dataSet(2).
parametersAndDataPair(8).
parameterSources(8,[return]).
dataTargets(8,[5,6,7,4]).

```

```

isInSecureWithRespectTo(guest)
+- accessibleParameters(guest,return(getId))
| +- linksDataAccessibleBy(guest,wireless)
| | +- linkAccessibleBy(guest,wireless)
| | | +- linkLocation(wireless) | | | '-
locationsAccessibleBy(guest)

```

**Palladio Component  
Model**

**Confidentiality Model**

**Prolog Prädikate**

**Analyse Ergebnis**

→  
Confidentiality4CBSE

→  
PCM2Prolog

→  
Haskalladio

- Daten werden in DataSets getrennt
- Information Flow ordnet Datenfluss an Operationen DataSets zu
  - Parameter
  - Rückgabewert
  - Aufruf der Funktion
  - Größe von Paramtern

ResourceContainer:

- Zusätzlich mögliche Verbindungen
- geteilt Laufzeitumgebung

LinkingResource:

- Welche Daten werden unverschlüsselt übertragen?

ResourceContainer + LinkingResource:

- Welche Maßnahmen (Tamper-Protections) wurden getroffen um Ressourcen zu schützen

- Welche DataSet dürfen bekannt sein?
- Welche Tamper-Protections kann/will der Angreifer umgehen?
- Wo hat der Angreifer Zugriff?

# Bisheriges Modell

## Profil-Mechanismus

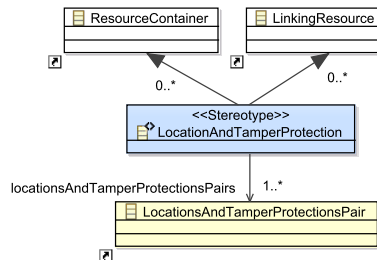
Confidentiality Modell:

- Definiert Klassen zum Modellieren von DataSet, Maßnahmen, Angreifer, ...

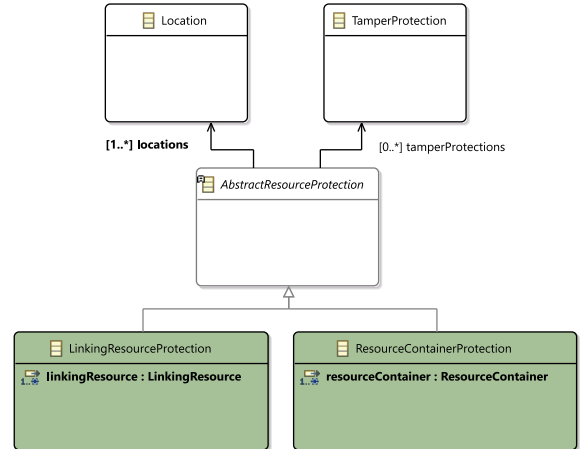
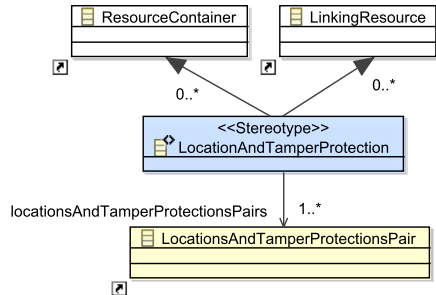
Confidentiality-Profil:

- Zusammenfassung von mehreren Stereotypen
- Stereotyp erweitert eine oder mehrere PCM Klassen
- Stereotyp hat Referenzen zu Elementen aus dem Confidentiality-Modell

→ soll entfernt werden

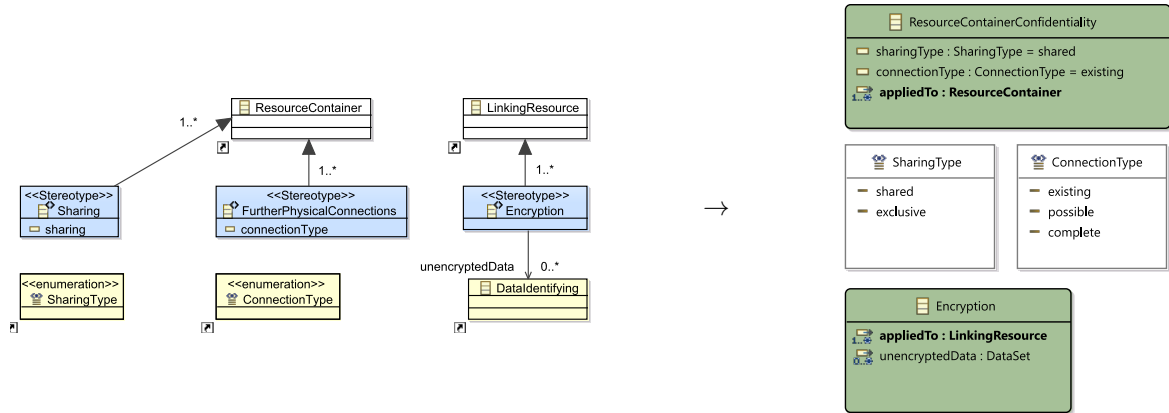


# Entfernen Profil-Mechanismus

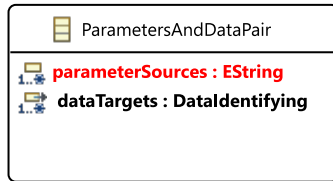




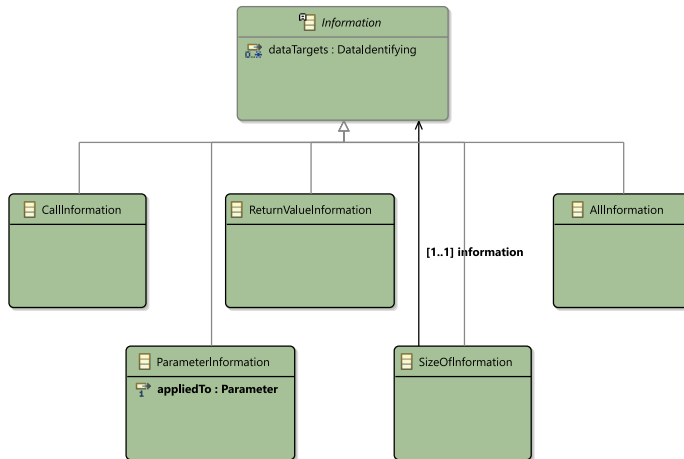
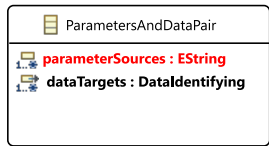
# Entfernen Profil-Mechanismus



- Zuordnung von DataSets und Datenflüssen an Operationen erfolgt über Strings
    - implizite Referenz
    - Verwechslungsgefahr bei gleichnamigen Parametern
- soll explizit modelliert werden

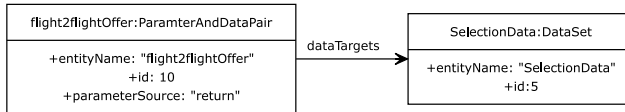


```
parameterSource = "requestData"  
parameterSource = "\return"  
parameterSource = "\call"  
parameterSource = "*"   
parameterSource = "sizeof(*)"
```



# PCM2Prolog

- xTend
- Reflective-API wird verwendet um Entitäten auf Prolog Prädikate abzubilden
- Filter bestimmt relevante Entitäten und Referenzen



→

```

parametersAndDataPair(10).
parameterSources(10,[return]).
dataTargets(10,[5]).
    
```

```

dataSet(5).
    
```

# Anpassungen PCM2Prolog

- Dispatch-Methoden für Entitäten die nicht automatisch generiert werden können

```
def dispatch String generateDeeplyCorrectly(EObject e) { return super.generateDeeply(e) }  
def dispatch String generateDeeplyCorrectly(AbstractResourceProtection rp) {...}
```

- Ursprüngliche Stereotypen Referenzen müssen umgedreht werden
  - Map<EObject,Set<String> > für jeden Stereotyp der auf PCM Komponenten angewandt werden kann
  - Beim Verarbeiten der neuen Klassen wird deren ID dem zur PCM Komponente gehörenden Set hinzugefügt
  - Nach dem alle Entitäten verarbeiten wurden → erzeuge Prädikate aus den Map Elementen

# Evaluierung

Modellierung der Beispiel Projekte `cloudscenario-minimized`<sup>1</sup> und `iflowexample`<sup>2</sup> 5 mit dem neuen Modell:

- Gleiche IDs verwenden

Automatischer Vergleich des Prolog Codes:

- Prolog Datei vorverarbeiten:
  - Listen innerhalb Prolog Prädikate sortieren: `prädikat(5, ["b","c","a"]).` wird zu `prädikat(5, ["a","b","c"]).`
  - Zeilen der Datei sortieren
  - Leerzeilen entfernen
- Ausgabe mit `diff` vergleichen

→ für diese Projekte möglich, aber nicht für alle möglichen Instanzen des ursprünglichen Modells

<sup>1</sup><https://github.com/KASTEL-SCBS/Examples4SCBS/tree/master/bundles/edu.kit.kastel.scbs.cloudscenario-minimized>

<sup>2</sup><https://github.com/KASTEL-SCBS/Examples4SCBS/tree/master/bundles/edu.kit.kastel.scbs.iflowexample>