View-Extraction for Annotating Models with Security Properties

Seminar

UNIVERSITÄT KOBLENZ · LANDAU

ist Institute for Software Technology

Marina Ernst

MSc Web Science

Supervisor: Sven Peldszus

Introduction

Motivation

Complexity

- software systems are critical
- they are becoming more complicated
- more complex approaches should be used on the early stages of development

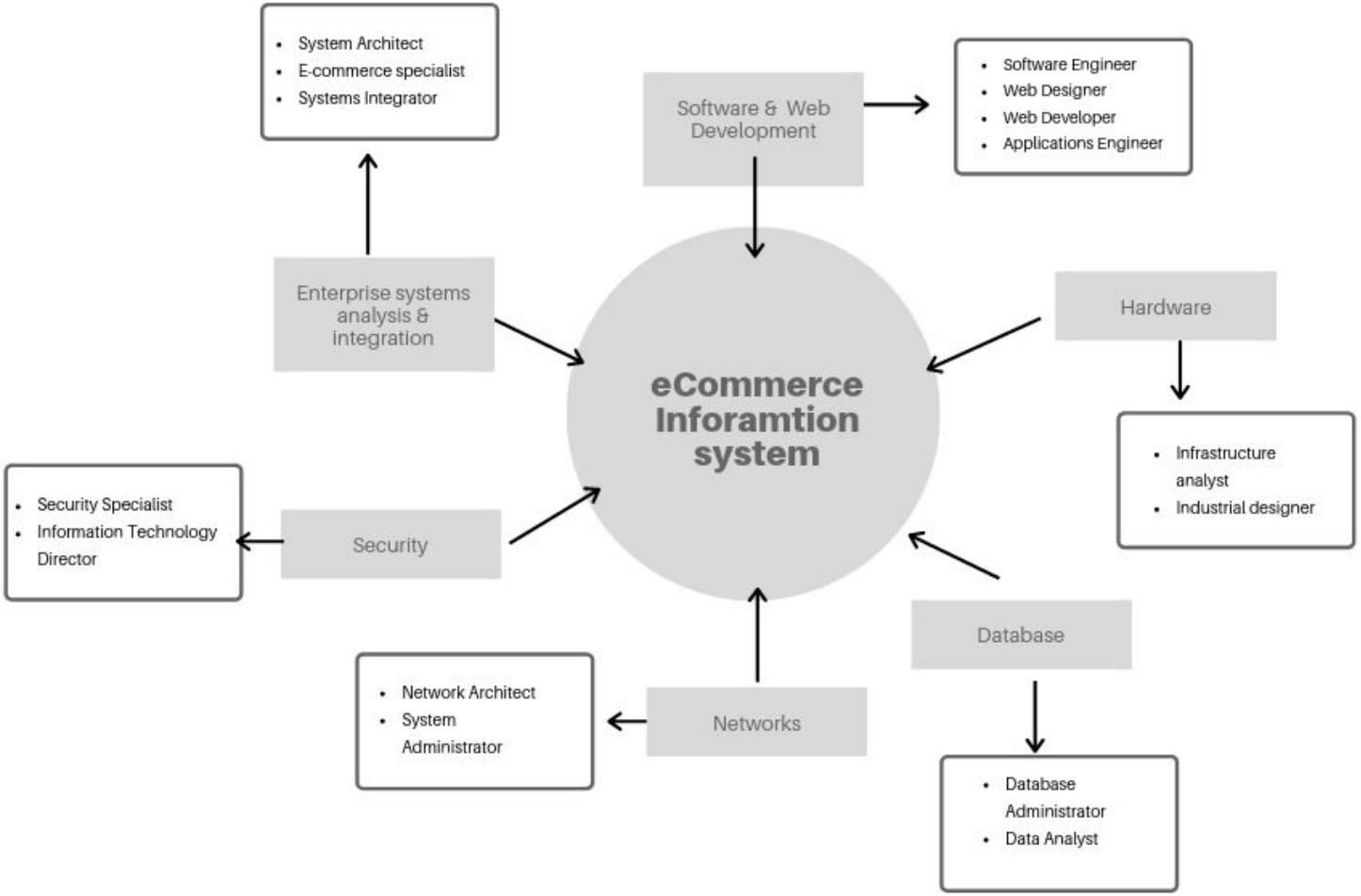
Security

- Security is a key factor
- Security requirements should be taking into consideration on earliest stages of developing
- More complexity in model as a result

What can be done???

View extraction

Example



IT-specialists interacting with eCommerce platform

Annotating models in software engineering

Annotating models in software engineering

First step in software engineering = requirements

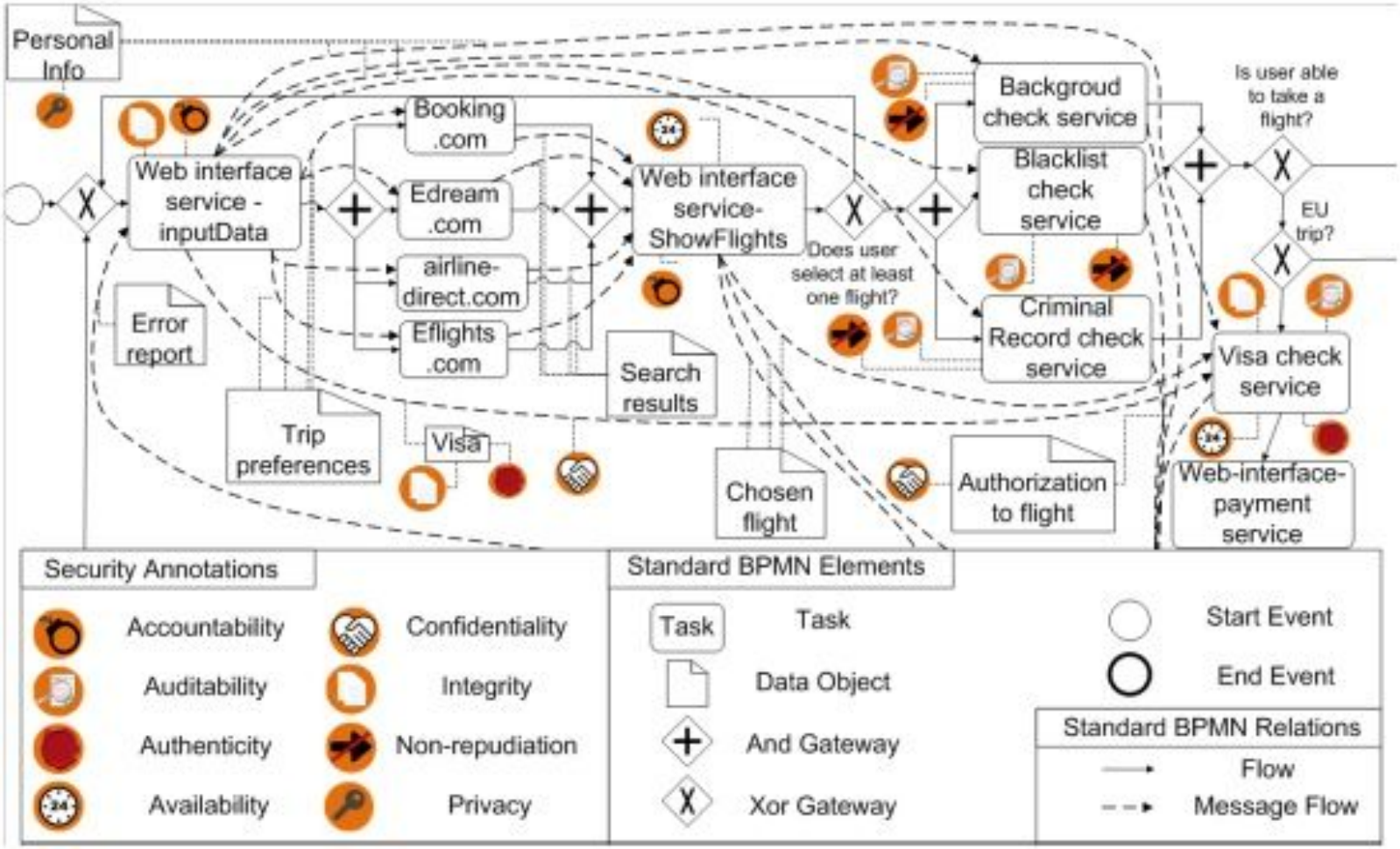
Annotating models = visual representation requirements

The most popular and well-known approaches are the following:

1. **UML** - Unified Modeling Language (UML)
2. **BPMN** - Business Process Model and Notation
3. **EPC** – Event-driven Processes chain
4. **IDEF** – ICAN Deffenition

BPMN with security properties

UNIVERSITÄT KOBLENZ · LANDAU
ist Institute for Software Technology



Example of a business process modeled using SecBPMN

BPMN with security properties

- A standard Business Process Model and Notation (BPMN) provides a simple means of communicating process information to other business users, process implementers, customers, and suppliers
- *The pure BPMN has no notation to represent the security properties.*

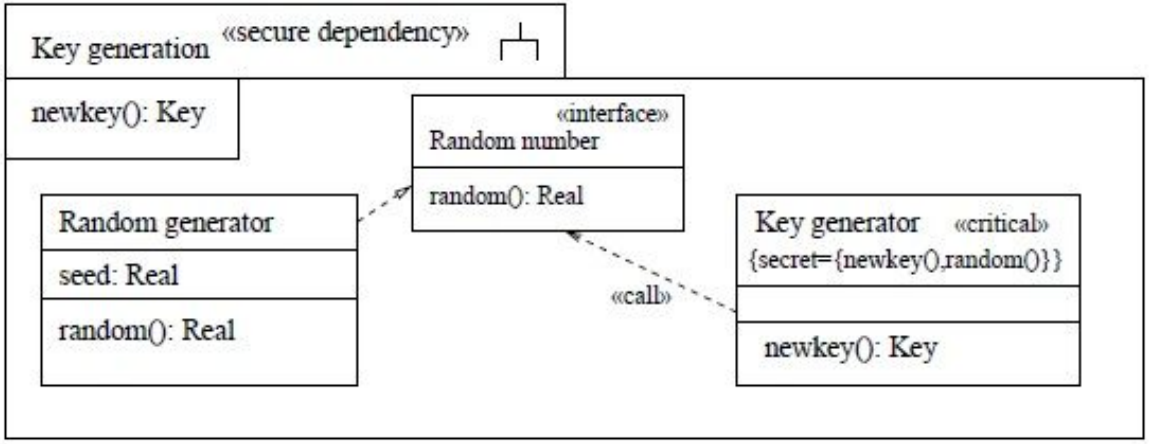
- Currently there is no unified approach BPMN-security, but there is a bunch of different methodologies, which allows to include security properties into BPMN such as:
  - BPMN Extension for the Modeling of Security Requirements [Rodriguez]
  - SecurityBPMN [Brucker]
  - Framework SecBPMN [Salnitri]

UMLsec

- The Unified Modeling Language (UML) is a visual modeling language, which is used to specify and document the artifacts of software system. Initially the main focus of UML is on object-oriented software systems, but nevertheless it'd also suitable for component-oriented systems
- UML includes several types of diagrams to provide an opportunity to model the software from different angle.

- *It has tools to visualize security properties of the system, because of the the UML standard itself.*
- In order to fulfill the these gaps and represent the Security related information in the UML diagrams the extension called **UMLsec** was invented by Prof. Jurjens in 2002

UMLsec



Example of UMLsec class diagram

- To construct UML extension one should collect definitions of stereotypes, tagged values and constraints and create a profile. In case of UMLsec profile consists of 21 stereotypes along with their tags and constraints

- The profile is constricted based on Security Properties namely:
  - Secrecy
  - Integrity
  - Authenticity
  - Freshness

Visual representation of large models

The impact of the size of the model

How the size of model can be measured?

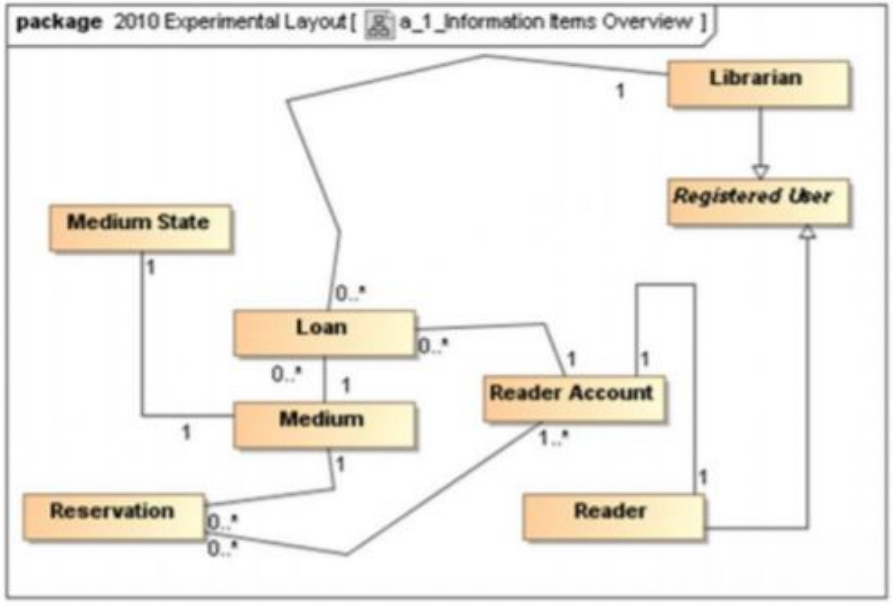
There are different approaches to measure the size of the model:

1. **Conceivable approach**
   It is based on counting the number of diagram elements.
2. **Pragmatic approach**
   A weight factor is introduced for the individual types of elements to compensate for differences between different element types

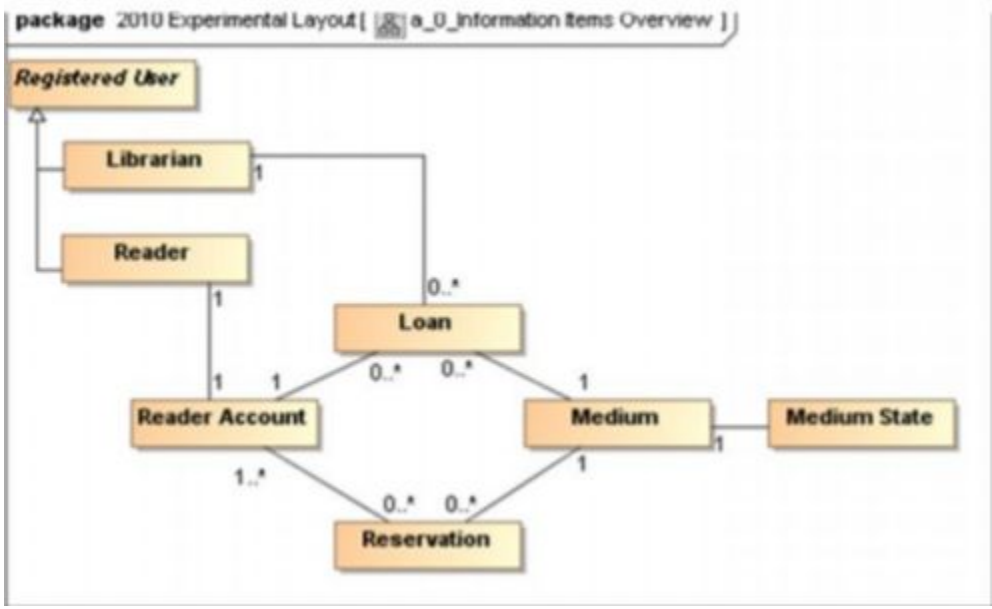
Problem: Understanding of large graphical models not only by machines, but also by humans

The impact of model layout

UNIVERSITÄT KOBLENZ · LANDAU
ist Institute for Software Technology



Bad layout



Good layout

Toy-example UML

The View extraction of annotating models

Clustering

Clustering is the process of grouping a set of objects in such a way that objects in the same group are more similar to each other than to those objects which are in other groups. Clustering is an unsupervised classification.

The clustering algorithm is categorized according to the technique it uses to cluster the data objects.

The various types of clustering algorithms are:

1. Hierarchical Clustering Algorithm
2. Partitioning Clustering Algorithm
3. Locality-based Clustering Algorithm
4. Grid-based Clustering Algorithm

Clustering

Result of clustering is representing the nested grouping of objects and similarity levels at which groupings change.

Challenge:
Clustering demands one element be only in one cluster.
It can be problem in case if the same element is relevant for two views.
Solution:
Define the most relevant for the task element as an initial element to start the algorithm

Additional problem:
Time complexity and memory consumption

Model Slicing

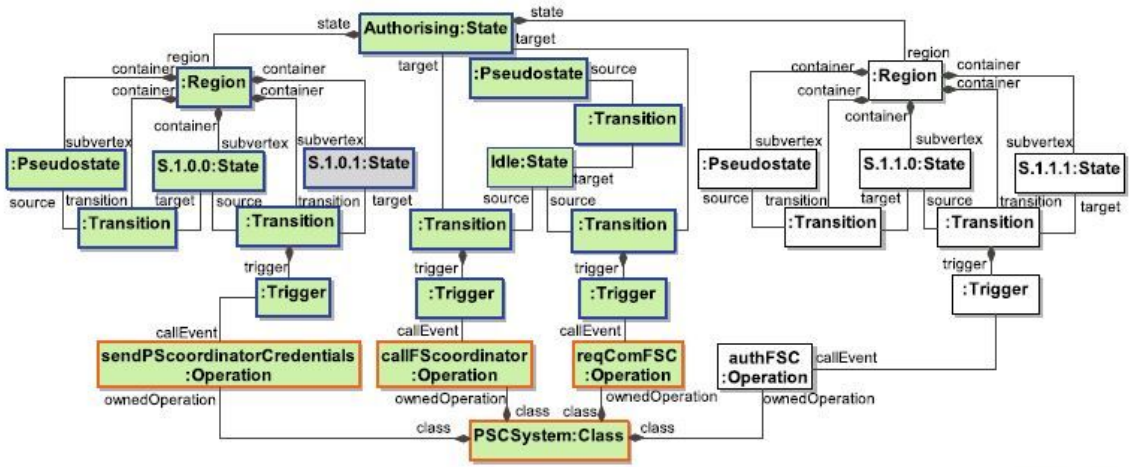
Model Slicing determines those parts of a program (the slice) which may affect the values of a set of (user-)selected variables at a specific point (the slicing criterion).

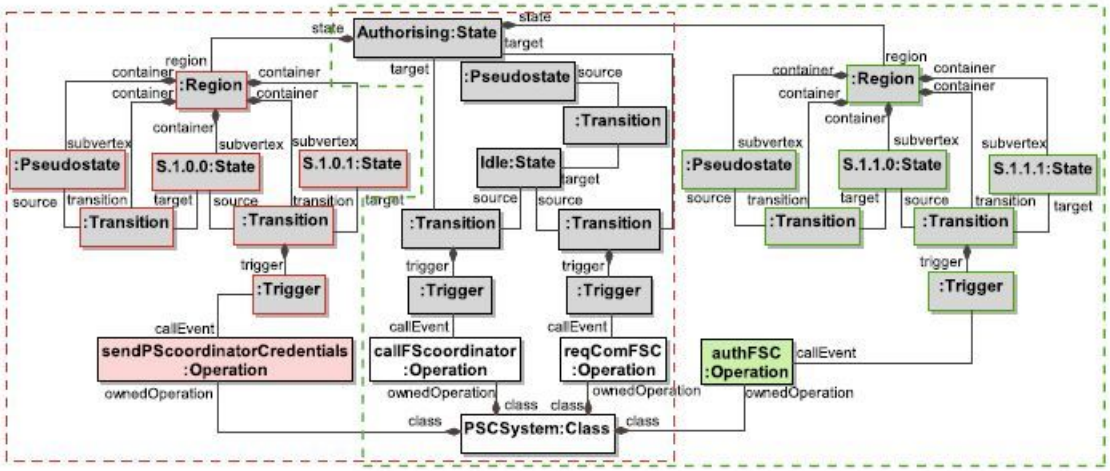
S = Slice(M,c)

*Slicing criterion **c** can be modified while working with the model*

Model Slicing

UNIVERSITÄT KOBLENZ · LANDAU
ist Institute for Software Technology





Excerpt of model slices (with different **c**)

Pietsch C. Kelter U. 27 Taentzer G., Kehrer T. A Formal Framework for Incremental Model Slicing.

Model Slicing

Challenge:
The value of the selected variables can be affected by a lot of other variables, which are also affected by some other elements, and so on. It might continue til the whole model become one slice.
Solution:

- define what is regarded as a dependency or effect.
- set up a limit for the distances between elements within one view.

Conclusion

Conclusion

Providing an appropriate level of Security and data protection in Information System is possible only by implementing security features in earliest stages of development.

In order to do so annotating models should be used.

Now only two modeling notating has an opportunity do include security accepts: BPMN and UML. But only UML has an extension UMLsec which is use for practical tasks.

Having Security Properties inside the models means that it should be possible to extract them along with whole model in understandable view and with an appropriate layout. The challenges in this case are the same as for the large model.

The general solution is decomposition of a model to smaller sub-models. There variety of methods to do this such as clustering or model slicing. Both can be appalled to UMLsec models as well as to UML without security properties.