

# Project proposal

## *1. Overall description of the project*

Today outsourcing plays an important role in the IT business domain. *Outsourcing* is the ongoing administration and management by an external party of specific (IT) processes to enhance their efficiency and effectiveness. The problem which arises while two entities (named client and a contractor) wish to collaborate is that after shifting its data the client does not longer control it and the data may be corrupted while processed by the contractor. To prevent undesirable losses caused by security breaches in contractor's security system (or at least to evaluate the possible losses) the client and the contractor sign a contract, named *PLA (Protection Level Agreement)*, where *quality of protection (QoP)* is specified and bounded by some indicators (metrics, appraisal). Example of such indicator is an average number of bad events which may happen while data is processed by the contractor.

The central question here is: *how the contractor should design a complex business process (BP) in order to achieve negotiated level of security (defined with some indicators).*

Before interaction with the client the contractor should define a concrete business process which must fulfill functional requirements (core functionality). However, there may be several alternative BPs which fulfill these requirements, but have different security levels. The contractor must decide which alternative is more secure and choose one concrete BP to be implemented/provided. Moreover, some activities of a BP are reoutsourced to other partners (called sub-contractors). There are may be several sub-contractors which are able to fulfill one activity. Furthermore, the contractor trusts each sub-contractor differently. This means that the contractor believes more that sub-contractor A will meet the negotiated requirements than sub-contractor B. Note, that the issue is very important since because of sub-contractor failure the process managed by the contractor may fail to satisfy agreed PLA with the client. Therefore, such notion as trust level of partner cannot be neglected.

We assume that the contractor knows the level of protection of each atomic activity in the process. It is true for such technology as Web Services when the contractor plays a role of orchestrator and he only invokes other services which *SLAs (Service Level Agreement)* are known. Since with each sub-contractor a PLA is specified the appraisals for each atomic activity in the process is known.

In order to aggregate security indicators of atomic activities and receive the value of the indicator for the complex process we use hypergraphs which is a generalization of AND-OR graphs. We need to transform a BP to the hypergraph, called Protection Appraisal DAG (PAD). The most secure concrete BP then will be the "shortest" hyperpath in such graph. When the hyperpath is found and its value is computed the most secure BP is recovered. An automatic tool is needed to support the theory and to carry out experiments (or simulation) which will prove the theory.

## 2. Description of the MSc Project

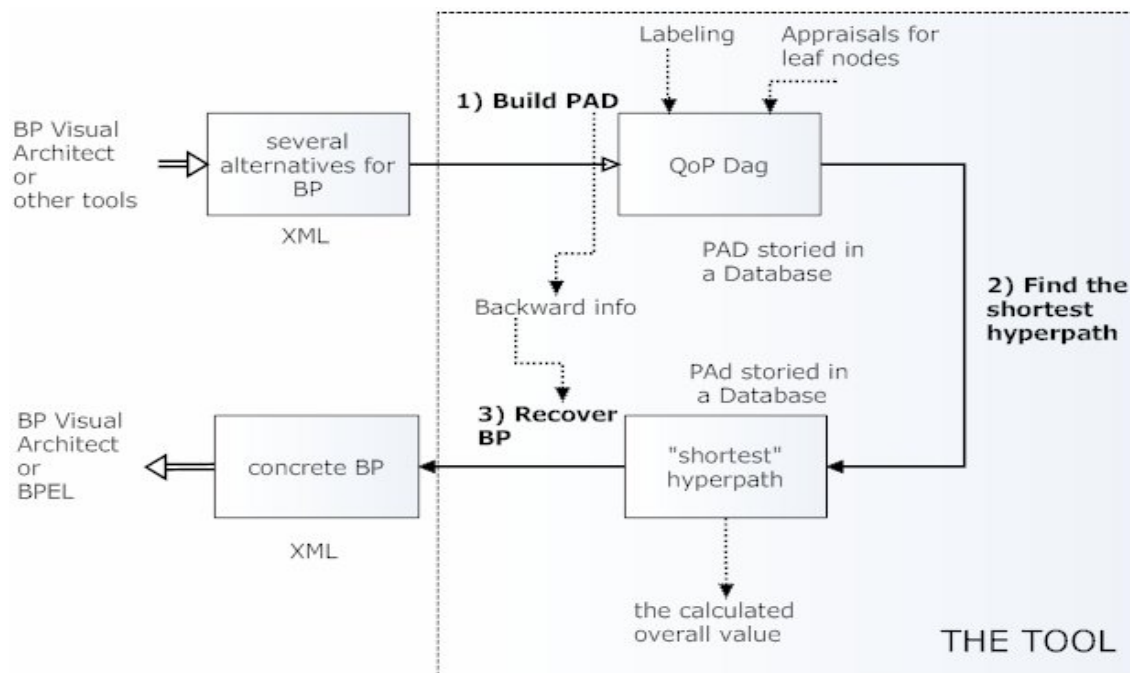
### 2.1. The goal

The goal of the project is to *create a tool* which chooses the most secure business process (BP) among various design alternatives. In other words, the student has to *implement* given algorithms and create a GUI for the analysis.

2.2 Objectives (roughly):

- 1) Map a designing business process (with several alternatives) to a Protection appraisal DAG (PAD).
- 2) Using the appraisals assigned to leaf nodes of the PAD find the “shortest” hyperpath to the top node.
- 3) Recover a business process (concrete BP) which corresponds to the hyperpath.

### High level workflow of the project.



0) Preliminary step. The work starts with designing of a business process which is created with BP Visual Architect 2.0 (BPVA). We introduce a new construct into the Business Process Modelling Notation (BPMN) which shows a design/deployment alternatives. Design/deployment alternative means that the same task may be fulfilled with different BPs/by different partners. The BP is stored in an XML file which can be considered as one of the inputs for the tool.

A preliminary analysis has been done on how to fetch the information from the XML file generated by BP Visual Architect 2.0. This information will be given to the student.

#### **Why BP Visual Architect 2.0?**

- *The tool provides all BPMN notation features.*
- *It is also possible to convert the BPMN to BPEL automatically with the tool.*
- *It contains quite complicated, but, on the first glance, readable XML file which can be used to start with.*
- *It also provides the possibility to create a new picture (“design alternative” box) and use it in the diagrams. Unfortunately, this is just a picture and cannot be treated as a BPMN construct: (i) this means that we cannot connect it to other constructs with a usual flow connector (but we can do it with another type of connector), (ii) the picture cannot be captured by the tool for automatic transformation to a BPEL diagram (naive thought but still...), and (iii) with it the BP diagram cannot be verified with the internal verifier.*
- *Also the BPVA 2.0 provides a very user-friendly interface and many useful features.*

- 1) The first thing the tool must do is to open the XML file and transform it into a PAD. This means that the student should be able to process the XML file and remove all information (around 90%) which is irrelevant for the task. Second, he should implement the algorithm for building a PAD. The algorithm already exists and will be provided to the student. The algorithm is written on an abstract level so the student should elaborate it but the main procedure must be left as it is (unless discussed and agreed). The tool also stores “Backward information” about business process required for its recovering. The obtained hypergraph (extracted from the XML file) will be stored in a database (one table for nodes and another for nodes). Some steps have been done in these directions and the results will be given to the student.
- 2) The tool should have a possibility to represent the graph graphically for further processing. Then we label the edges and nodes of a PAD (by assigning weights and definitions of the propagation functions) and define appraisals for leaf nodes. This task should be done in both ways: (i) manually, through GUI, and (ii) uploaded from files. The tool also should be able to store the PAD (the two tables), its weights, assigned functions and premise appraisals in separate files (or as a project).
- 3) Then the tool should use an algorithm for the calculation of the “shortest” path. The algorithm also exists and will be given to the student. This method should be presented as a plug-in (module) so that other methods for “shortest path calculation” can be used if it will be needed in the future. The method returns a hyperpath (or concrete BP in other words) and a final aggregated value.
- 4) The last step is to recover the concrete BP which corresponds to the found hyperpath and transform it into the XML format understandable for BP Visual Architect 2.0 or in BPEL format.
- 5) On-line feature. The tool should support dynamic changes in the hypergraph: e.g., if some small changes occurred (a weight has been changed, a node has been deleted) the tool should efficiently recalculate the “shortest hyperpath”. The algorithm for the case will be provided.

- 6) Some more features may be added or removed during the project (e.g., asset-oriented view).

The student is free to provide any suggestions which will make the tool and the theory itself more efficient and complete. Moreover, during the collaboration a paper (or more) may be written and submitted to a conference/workshop/journal.

### ***3. Required Expertise:***

- 1) Programming skills (Java or C++) (good);
- 2) XML (average, to be able to read it);
- 3) Business Process (to be familiar with it).
- 4) Graph theory (average).
- 5) Databases (average).
  
- 6) Knowledge of BPMN, BPEL, Hypergraphs, Security of BP, Web Services (the project may drift in this direction) is welcome.

### ***4. Background reading***

- 1) Papers about the project:
  - a) F. Massacci and A. Yautsiukhin. **Modelling of quality of protection in outsourced business processes**. In *Proceedings of the The Third International Symposium on Information Assurance and Security*. IEEE Press, To appear., 2007.  
<http://dit.unitn.it/~evtiukhi/Resources/MASS-07-IAS.pdf>
  - b) F. Massacci and A. Yautsiukhin. **An Algorithm for the Appraisal of Assurance Indicators for Complex Business Processes**. In *Proceedings of the The Third Workshop on Quality of Protection*. To appear., 2007.  
<http://dit.unitn.it/~evtiukhi/Resources/MASS-07-QoP.pdf>
  
- 2) Papers about hypergraphs and hyperpaths (with algorithms):
  - a) G. Ausiello et al. Optimal traversal of directed hypergraphs. Technical Report TR-92-073, International Computer Science Institute, Berkeley, CA, 1992.  
<http://citeseer.ist.psu.edu/387736.html>
  - b) G. Gallo, G. Longo, S. Pallottino, and S. Nguyen. Directed hypergraphs and applications. *Discr. App. Math.*, 42(2-3):177–201, 1993.  
<http://www.cis.upenn.edu/~lhuang3/wpe2/papers/gallo92directed.pdf>
  
- 3) Papers about business process:
  - a) BPMN  
<http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf>

- 4) BP Visual Architect

A trial version of BP Visual Architect can be downloaded from:

<http://www.visual-paradigm.com/product/bpva/>

## ***5. Contact information***

Person: Artsiom Yautsiukhin

e-mail: [evtiukhi@dit.untin.it](mailto:evtiukhi@dit.untin.it)