

# A General framework for security-aware analysis of services

Leanid Krautsevich, Fabio Martinelli  
and Artsiom Yautsiukhin

# Outline

- Motivation
- Graph Building
- Semirings
- Analysis of the process
- Interoperability
- Conclusion

# Motivation

- Many security metrics and trust metrics for assessment
- Services are composed in run-time and security and trust must be taken into account
- Provide a uniform framework for analysis of different metrics.

# Goal

## ■ Context:

- We have a business process with a number of atomic processes.
- There are different alternatives
- Each process has some value for a security metrics

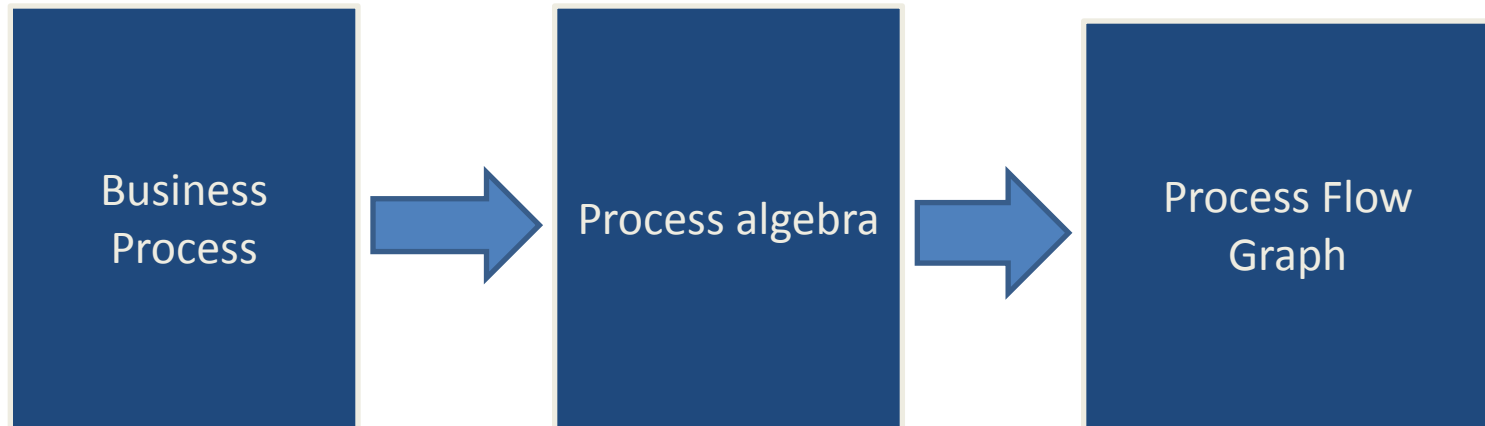
## ■ We want:

- To get the overall value
- Select the best alternative process
- Do this in the most general way.

# BPMN, BPEL, and ...

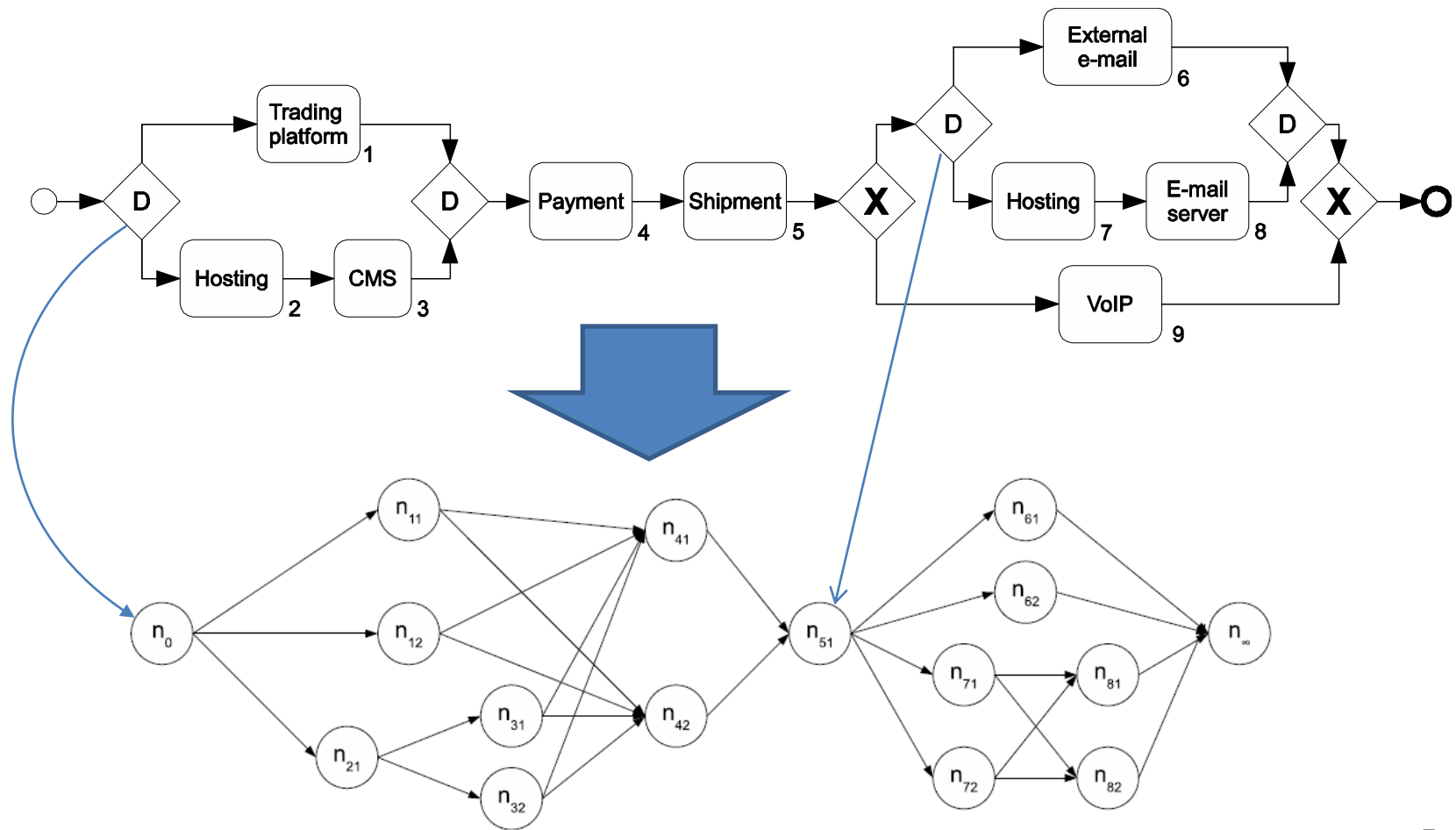
- BPEL
  - Formal (XML-based)
  - Low level (execution)
- BPMN
  - Informal (just diagrams)
  - High level (design)
- Process algebra?
  - $P, Q = 0 \mid a \mid Q.P \mid P \parallel Q \mid P+Q$

# Transformation of BP to a tree



- Deterministic vs. non-deterministic choice
- BPMN and BPEL do not have design choice!  
We need it.

# Transformation of BP to a tree



# Semirings

- $S = \langle A, \oplus, \otimes, \mathbf{0}, \mathbf{1} \rangle$
- $A$  is a set of elements and  $\mathbf{0}, \mathbf{1} \in A$
- $\oplus$  - additive operation over  $A$ .
  - Commutative
  - Associative
  - $\mathbf{0}$  – its unit element.  $a \oplus \mathbf{0} = a = \mathbf{0} \oplus a$
  - If  $a_1 \leq a_2$  then  $a_1 \oplus a_2 = a_2$
- $\otimes$  - multiplicative operation over  $A$ .
  - Distributive over the additive operation
  - $\mathbf{1}$  – its unit element.  $a \otimes \mathbf{1} = a = \mathbf{1} \otimes a$
  - $\mathbf{0}$  - its annihilator:  $a \otimes \mathbf{0} = \mathbf{0} = \mathbf{0} \otimes a$

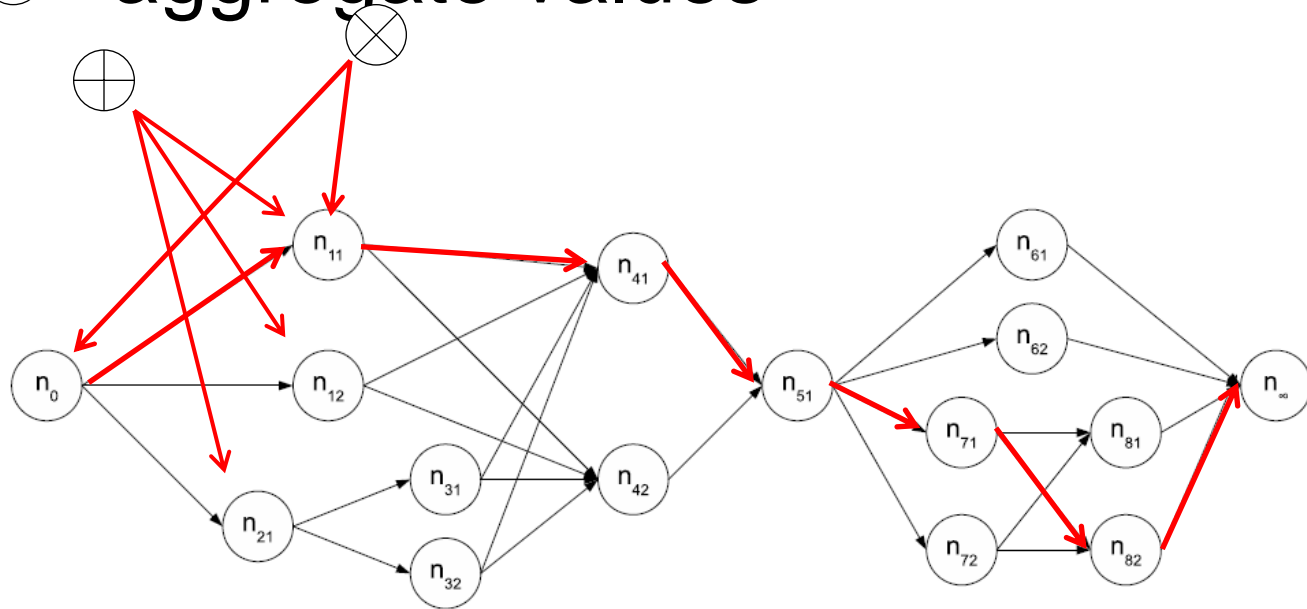
# Security metrics as semirings

- Risk =  $\langle \mathbb{R}^+, \min, +, \infty, 0 \rangle$ 
  - $\min()$  – associative and commutative
  - $\min(a, \infty) = a$
  - $+$  - distributive over  $\min$
  - $a + 0 = a$
  - $a + \infty = \infty$
  - If  $a_1 \geq a_2$  then  $\min(a_1, a_2) = a_2$
- Probability of attacks, trust =  $\langle [0, 1], \max, \times, 0, 1 \rangle$
- Minimal number of attacks =  $\langle \mathbb{N}^+, \min, +, \infty, 0 \rangle$
- Downtime =  $\langle \mathbb{R}^+, \min, \max, \infty, 0 \rangle$

# Use of semirings

■  $\oplus$  - select the best alternative

■  $\otimes$  - aggregate values



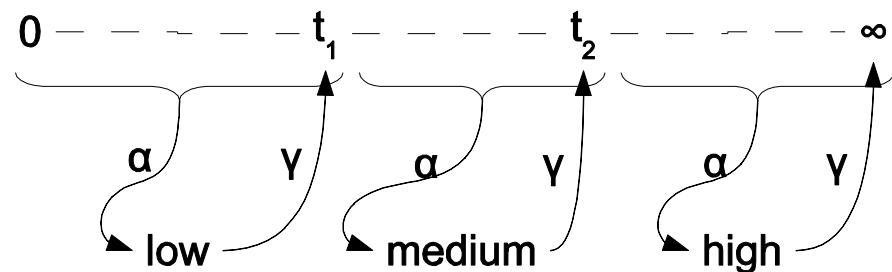
# Analysis

- Problems:
  - Find the best case (the best BP)
  - Find the worst case (the BP which can be guaranteed)
  - Selection of concrete services
  - ...
- Solutions for semirings already exist.

# Interoperability

- Quantitative  $\langle R^+, \min, +, \infty, 0 \rangle$
- Qualitative  $\langle D, +', x', \mathbf{0}, \mathbf{1} \rangle$ 
  - $D = \{\text{high, medium, low}\}$
  - $+' = \text{high} < \text{medium} < \text{low}$
  - $x' = \text{risk matrix}$
  - $\mathbf{0} = \text{high}, \mathbf{1} = \text{low}$

Quantitative risk:



Qualitative risk:

# Conclusion

- Semirings is a useful technique for general assessment of BP
- Semirings help to perform various types of analysis
- Semirings also may help to analyse BP when different metrics are used

# Future work

- Improve the transformation process in order to deal with non-deterministic choice.
- Consider data flow together with workflow.
- Consider different types of analysis applicable for semirings
- Investigate deeply interoperability relations between various metrics

# Questions?

# Galois insertions

- Let  $(C, \subseteq)$  and  $(A, \leq)$  be two posets
- $\langle \mathbf{a}, \mathbf{y} \rangle = (C, \subseteq) \Leftrightarrow (A, \leq)$  are maps:
  - $\mathbf{a}: C \rightarrow A$  ;
  - $\mathbf{y}: A \rightarrow C$  ;
- $\mathbf{a}$  and  $\mathbf{y}$  are monotonic ;
- for each  $x \in C$ ,  $x \subseteq \mathbf{y}(\mathbf{a}(x))$
- for each  $z \in A$ ,  $\mathbf{a}(\mathbf{y}(z)) \leq z$