Secure Service Composition Adaptation Based on Simulated Annealing

Liverpool John Moores University, UK

Bo Zhou

B.Zhou@ljmu.ac.uk

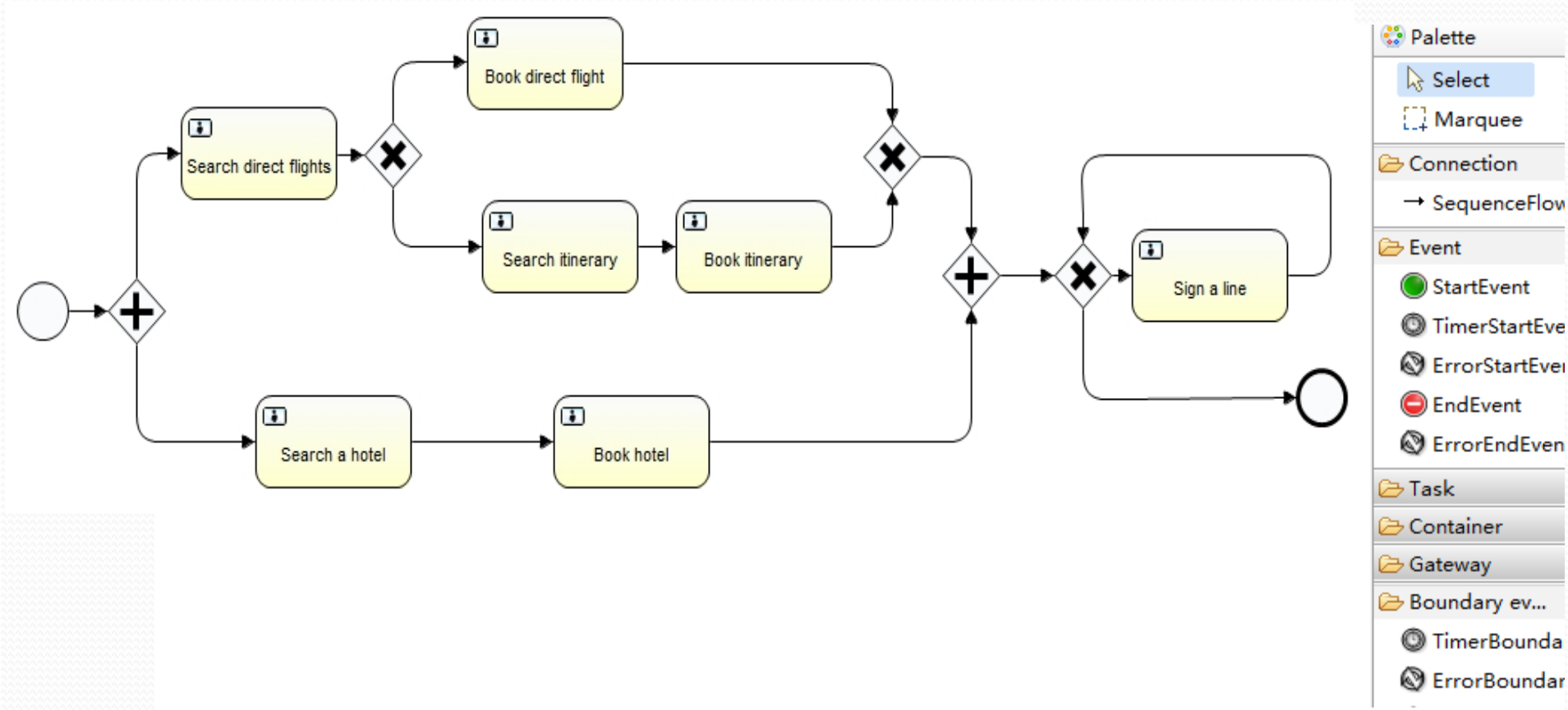
Talk Overview

- SOA and its security issues
- Secure service composition adaptation
- NP-complete
- Heuristic method
- Simulated annealing

Service-oriented Architecture

- Foundation for modelling, planning, searching for and composing services.
- Offer new applications via composition of services.
- Facilitated by standardised interoperations among services.
  - WSDL, USDL, BPMN

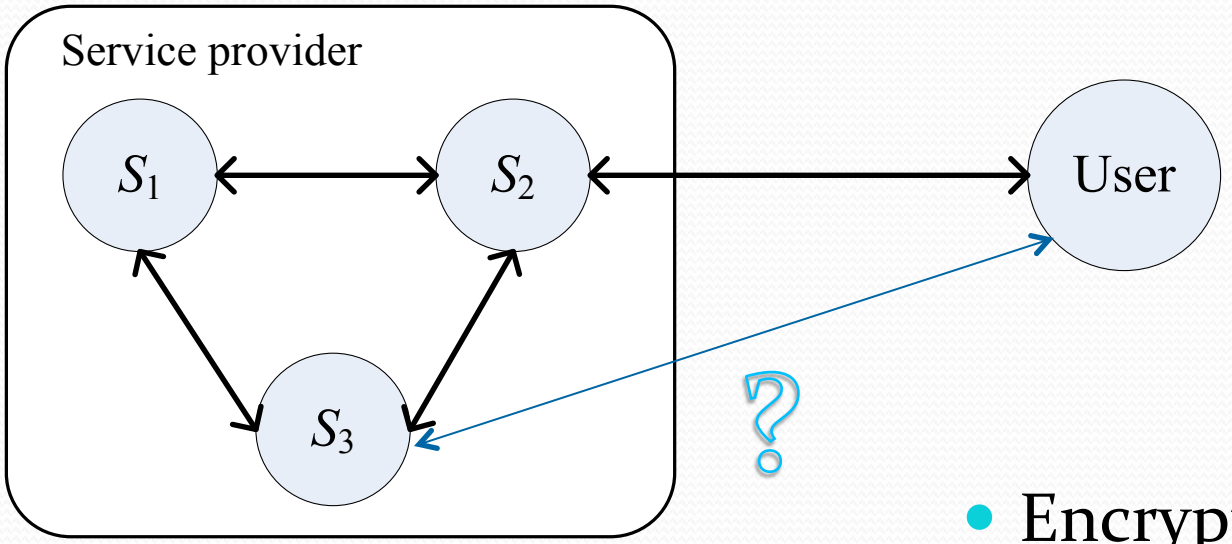
A BPMN example



Security issues in SoA

- Different provider
- Inconsistency in security policy
- Change of context
- Change of requirements
- New threats

Dynamic Security Requirements



- Encryption?
- SQL injection?
- Non-delegation?
- ?...

Security measures in SOA

- Verification is to ensure selected services comply with the security policy at both design- and run-time.
  - There are variety of existing tools for performing analysis of individual or composed services. i.e. formal analysis and code analysis

- Inconsistent security policies and configurations must be continually monitored and addressed.
  - Countermeasures such as adaptation or recomposition.

Secure Service Composition Adaptation

- Composition adaptation aims to mitigate issues identified during verification and monitoring.

- Adaptation is not straightforward due to the following reasons.
  - No direct suggestions from verification tools.
  - Concept of security is broad.
  - A simple substitution of a service may result in dramatic changes to the security properties of the entire composition.
  - Individual success does not guarantee collective satisfactory. For example, two services use different encryption algorithms.

- The secure composition adaptation issue is actually an optimisation problem with constraints.
  - Especially when facing wide choice of alternatives.

Heuristic Solutions

- Solving problems that have no polynomial-time algorithms are known.
  - 0/1 Knapsack, traveling salesman
- Exhaustive search is impractical.
  - Verification could be a time and resource consuming process
- Heuristic methods make choices`intelligently‘, attempting to find increasingly successful solutions until an adequate answer is found.
  - Aiming for fast and accurate adaptation.

Proof of NP-Completeness

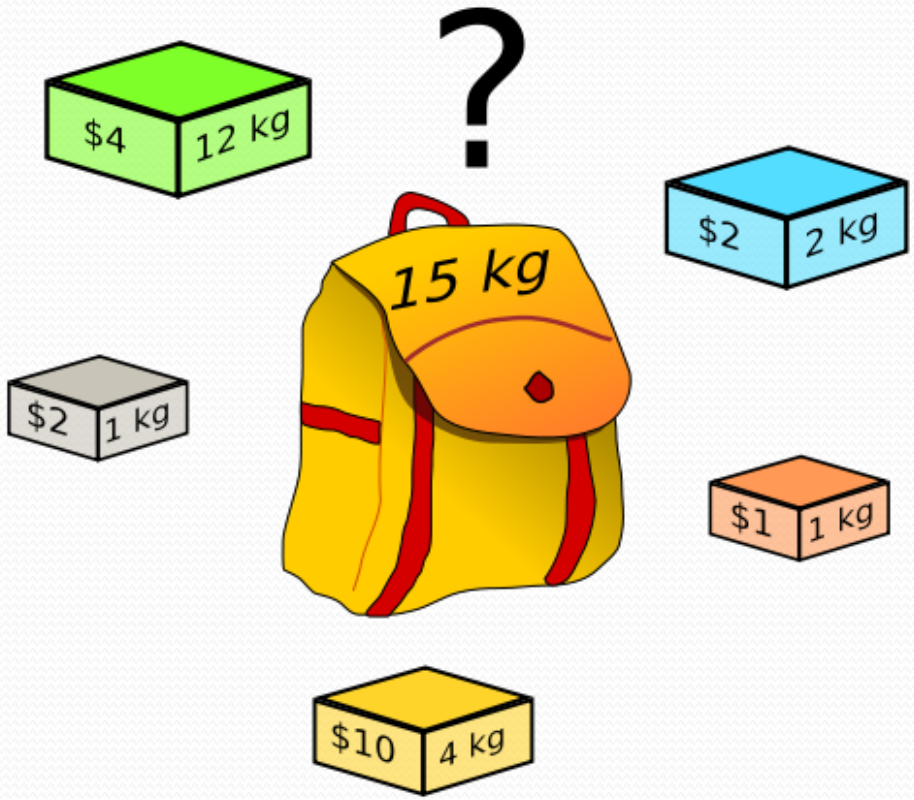
- By definition , a decision problem D is NP-complete if
  - D is in NP (Nondeterministic Polynomial time), and
    - With the help of verification techniques, candidate adaptation solution can be verified in polynomial time.
  - Every problem in NP is reducible to D in polynomial time.
    - We need to prove Secure Service Composition Adaptation is at least as hard as any known NP-complete problem.

The 0/1 Knapsack Problem

Given a set of items, each with a weight and a value, determine the items to be included in a combination so that the total weight is less than or equal to a given limit (e.g. the capacity of a knapsack) and the total value is as large as possible.

- Sartaj Sahni, "Approximate Algorithms for the 0/1 Knapsack problem," Journal of the ACM, vol. 22, no. 1, pp. 115-124, January 1975.

The 0/1 Knapsack Problem



$$\max V = \sum_{i=1}^{n} v_i x_i,$$

$$\text{subject to} \quad \sum_{i=1}^{n} w_i x_i \leq W,$$

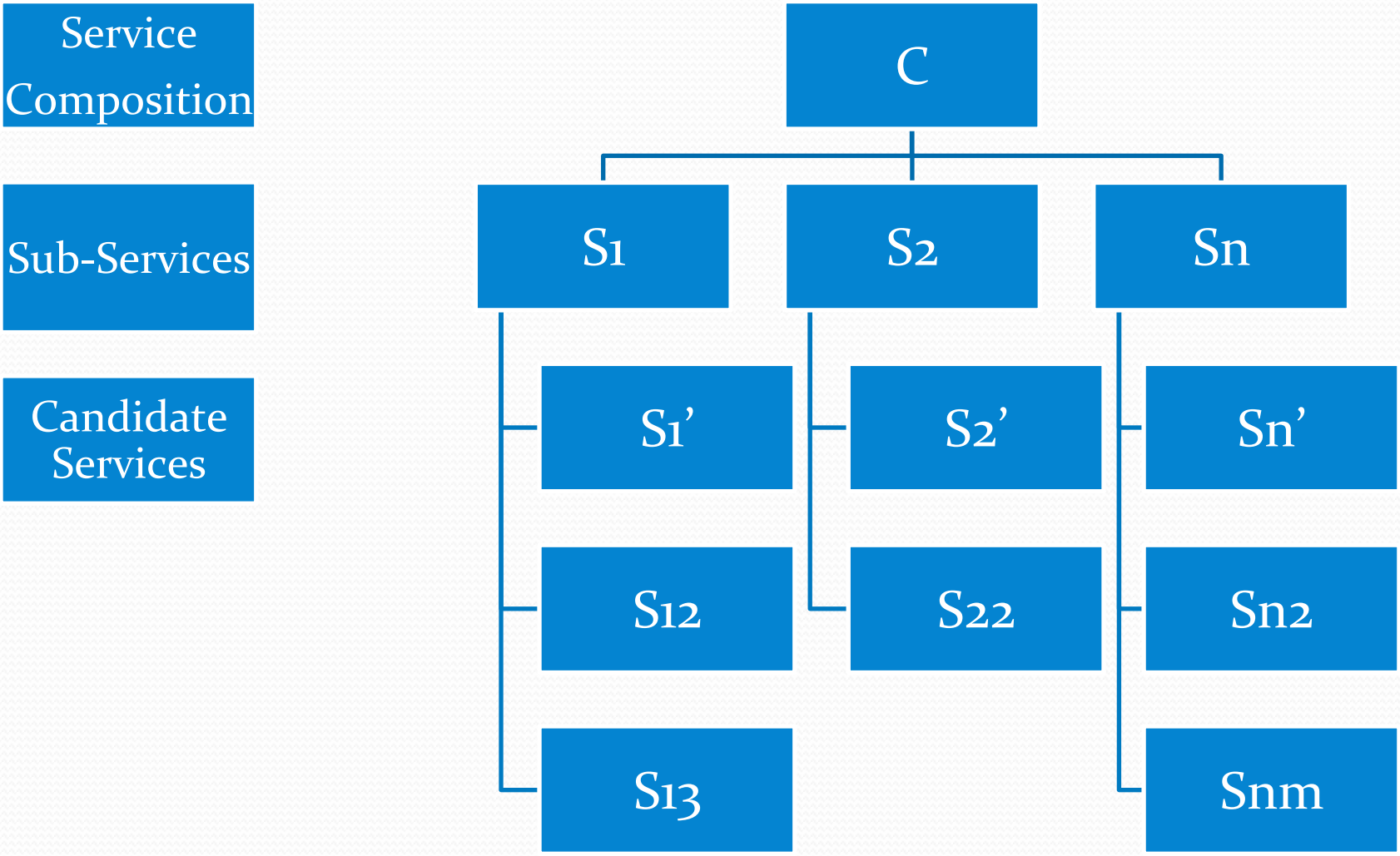
$$\begin{aligned} \text{where } n &= \text{number of items;} \\ v_i &= \text{value of item } i; \\ w_i &= \text{weight of item } i; \\ x_i &\in \{0, 1\}. \end{aligned}$$

Similarity to our problem

- Definition- Given a set of alternative services, what is the best combination of them in order to achieve the most secure service composition?
- There are always constraints while selecting services.
  - On trustworthiness, running efficiency and many other QoS and security related factors.
- Focus on typical business decision where the user has to balance security with cost.

Cost->Weight Security->Value

The Most Simple Case



Same Mathematical Complexity

- Given an alternative composition, is it securer than the most secure one previously known, while remaining within the user's budget?

$$\max S = \sum_{i=1}^{m} (s_i' - s_i) x_i,$$

$$\text{subject to} \quad \sum_{i=1}^{m} (p_i' - p_i) x_i \leq P,$$

where m = number of services in C;

$s_i' - s_i$ = change of security if service i replaced;

$p_i' - p_i$ = change of price if service i replaced;

P = threshold value determined by user's budget;

$x_i \in \{0, 1\}$, decision virable with service i.

Simulated Annealing

- Used to solve NP-complete problems in general, including 0/1 knapsack problem.

- Named to mimic the chemical process when atoms in metal become placed in relative order during the process of being overheated to gradually being cooled.

The Solution

- 1. Choose a feasible list of services that can be replaced randomly.
- 2. Randomly select a service from the original composition.
- 3. If the service has not been included in the list for replacement, add the service to the list. Randomly choose alternative services from service pool for each service on the list and form a new composition. If the new composition does not satisfy the cost constraint,
- randomly remove a service from the replacement list until it becomes feasible.
- 4. While in step 3 if the service has already been selected, remove this service from the list and pick up another service from the original composition. Randomly choose alternative services to form a new feasible composition.
- 5. If the new composition satisfies equation 5, as well as passing the security verification test, than the new composition will be accepted:

$$e^{\frac{\Delta S}{T}} > R(0,1)$$

  where S represents the change of security impact value calculated based on equation 4, T is the simulated temperature value that confines the optimisation process, e is the mathematical constant and R(0; 1) generates a random number between 0 and 1.
- 6. Let S be the security impact value. If S is a positive, this means the new composition has a higher security score and equation 5 is always true; if S is negative, than the new composition has lower score. However, it is still possible that the new composition with negative S can be accepted. In effect, with larger T, the chance of satisfying equation 5 is higher.
- 7. Repeat steps 2-6 several times decreasing T at each step until a lower threshold for the value of T is reached.
- 8. When T reaches the threshold value, the current solution will be the best one we can get.

Quantify Services

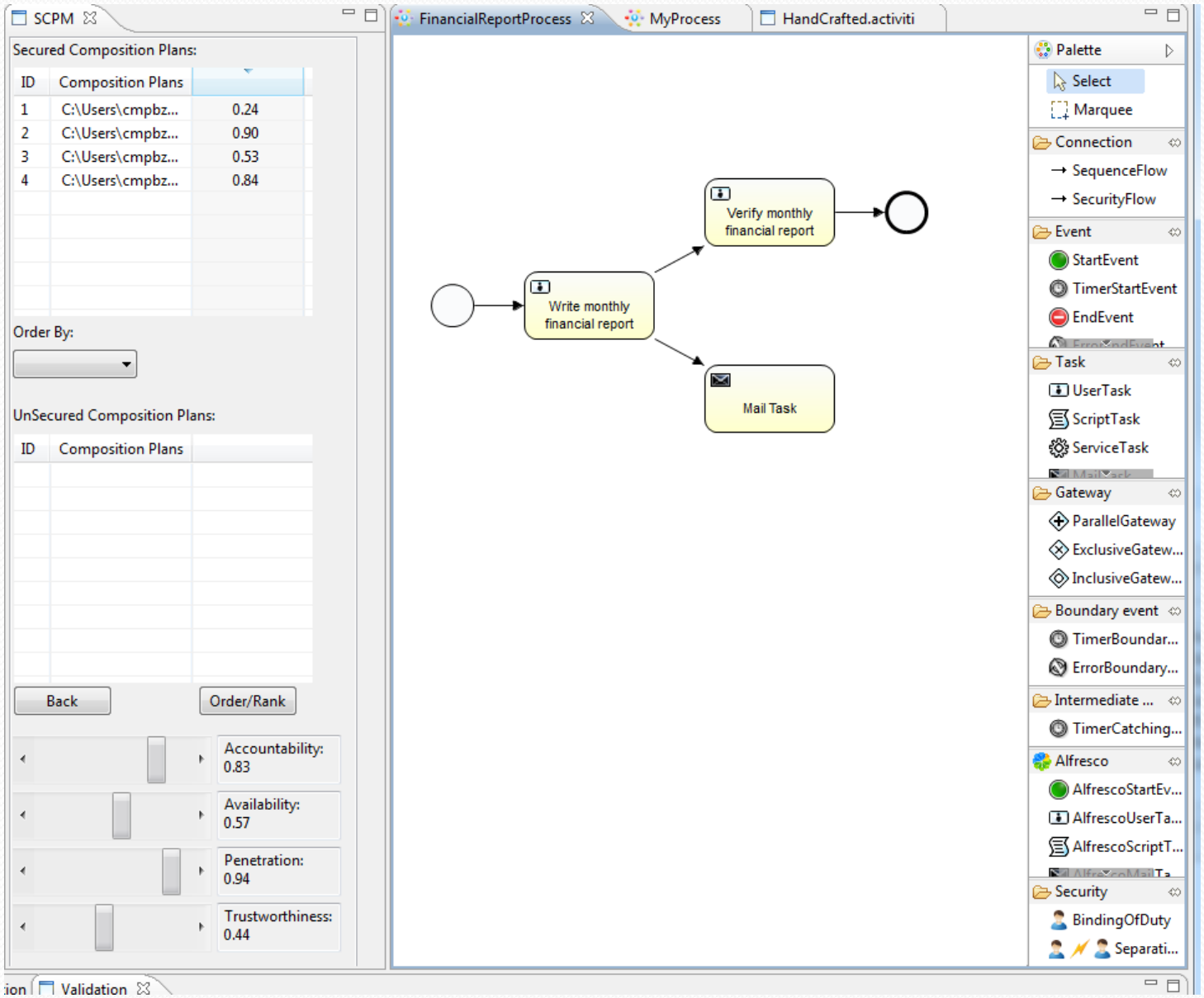
- To apply the solution, we have to find away to quantify services.
  - Allow direct comparison of services.
- Current proposal is to measure the services based on three criteria.

$$S = 0.3 \times V + 0.2 \times A + 0.15 \times T$$

where V = Availability,

A = Accountability,

T = Trustworthiness,


SCPM
Secured Composition Plans:
ID
Composition Plans
1
C:\Users\cmpbz...
0.24
2
C:\Users\cmpbz...
0.90
3
C:\Users\cmpbz...
0.53
4
C:\Users\cmpbz...
0.84
Order By:
UnSecured Composition Plans:
ID
Composition Plans
Back
Order/Rank
Accountability: 0.83
Availability: 0.57
Penetration: 0.94
Trustworthiness: 0.44
Validation
FinancialReportProcess
MyProcess
HandCrafted.activiti
Verify monthly financial report
Write monthly financial report
Mail Task
Palette
Select
Marquee
Connection
SequenceFlow
SecurityFlow
Event
StartEvent
TimerStartEvent
EndEvent
Task
UserTask
ScriptTask
ServiceTask
Gateway
ParallelGateway
ExclusiveGatew...
InclusiveGatew...
Boundary event
TimerBoundar...
ErrorBoundary...
Intermediate ...
TimerCatching...
Alfresco
AlfrescoStartEv...
AlfrescoUserTa...
AlfrescoScriptT...
Security
BindingOfDuty
Separati...

Aniketos Project at LJMU

- EU (FP7/2007-2013) funded project (grant no. 257930).
  - The project includes 17 partners from 10 different European countries.
  - Period: Aug 2010 – Jan 2014 (42 months duration).
- Aiming to achieve
  - Provide service developers and providers with a **secure service development framework** that includes methods, tools and security services that supports the design-time creation and run-time composition of secure dynamic services, where both the services and the threats are evolving.
  - Visit http://aniketos.eu for more info.

Future Work

- Examine the efficiency of Heuristics solutions
  - Adaptation speed and accuracy
  - Other solutions apart from Simulated Annealing
  - Refine the quantification criteria

Summary

- Service composition is not always secure
- Secure service composition adaptation is needed to address secure issues
- The problem is a NP-complete, reducible to 0/1 knapsack problem
- Heuristic solutions such as Simulate Annealing is applied
- More work needed for quantification of services

Q & A