Multi-dimensional Secure Service Orchestration

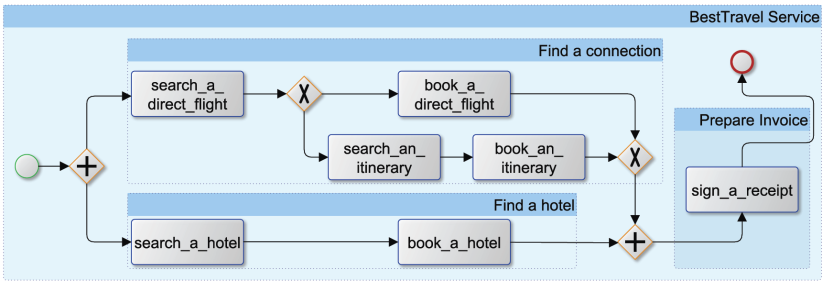
Gabriele Costa, Fabio Martinelli, and
Artsiom Yautsiukhin

NESSoS Bertinoro 2013

Outline

- Quantitative aspects in Secure Service Composition
  - Running example
  - Syntax of history expressions
  - Semirings
  - Galois insertions
  - Aggregation of metrics
  - Abstraction of metrics
- Conclusions

Running example. Process.



- BestTravel creates an abstract BP
- Concrete candidates are determined -> a number of composition plans exist.
- Goals: find composition such that:
  - Risk levels of find a connection and find a hotel less than 75 euro
  - Trust rating of find a connection and find a hotel – not lower than 0.8
  - Time of recovery of find a connection and find a hotel is lower than 120 minutes

Running example. Marketplace

Abstract	Index	Concrete	Risk	Trust	Recovery Time
Search a direct flight	1	Windjet	10	5	75
	2	Ryanair	20	4	45
Search an itinerary	3	Lufthansa	5	0.98	Fast
	4	Airfrance	8	0.05	Normal
Booking service	5	Paypal	5	0.95	30
	6	Ripplepay	15	0.85	60
Search a hotel	7	HotelBooker	40	0.93	60
	8	HotelClub	30	0.92	90
Sign a receipt	9	ESignForms	0.3; 0.6; 0.9	0.73	150
	10	VeriSign	0.4; 0.5; 0.8	0.87	200

Overall procedure

1. Formalise a process
2. Add concrete services instead of abstract ones.
3. Assign metrics to specific services
4. Aggregate metrics and identify the worst/ best alternatives
5. Check whether aggregated values satisfy the requirements

Syntax of history expressions

History expressions H, H’	ε	Void
	h	Variable
	a(r)	Security-relevant action (on target r)
	H + H’	Union
	H · H’	Concatenation
	H | H’	Parallel execution
	d#H	Metric-annotation
	φ[H]	Policy framing (φ applied on service security agreement H)
	γ<H>	Metric check
	μh.H	Recursion

Example. Process and metrics

Find a connection — Find a hotel

$$H_{BT} = \left(\gamma \left\langle (H_1 + H_2) \cdot \left(\begin{array}{c} (H_5 + H_6) \\ + \\ ((H_3 + H_4) \cdot (H_5 + H_6)) \end{array} \right) \right\rangle \middle| \gamma \left\langle \begin{array}{c} (H_5 + H_6) \\ \cdot \\ (H_7 + H_8) \end{array} \right\rangle \right) \cdot \gamma \langle \mu h.((H_9 + H_{10}) \cdot h + \varepsilon) \rangle$$

Sign a receipt

$H_1 = d_1 \# H_1' = (10, 5, 75) \# H_1'$	$H_6 = d_6 \# H_6' = (15, 0.89, 60) \# H_6'$
$H_2 = d_2 \# H_2' = (20, 4, 45) \# H_2'$	$H_7 = d_7 \# H_7' = (40, 0.93, 60) \# H_7'$
$H_3 = d_3 \# H_3' = (5, 0.98, \text{fast}) \# H_3'$	$H_8 = d_8 \# H_8' = (30, 0.92, 90) \# H_8'$
$H_4 = d_4 \# H_4' = (8, 0.95, \text{normal}) \# H_4'$	$H_9 = d_9 \# H_9' = ((0.3; 0.6; 0.9), 0.73, 150) \# H_9'$
$H_5 = d_5 \# H_5' = (5, 0.95, 30) \# H_5'$	$H_{10} = d_{10} \# H_{10}' = ((0.4; 0.5; 0.8), 0.87, 200) \# H_{10}'$

c-semirings

- S=<D, $\oplus$, $\otimes$, **0**, **1**>
- D is a set of elements and **0,1** $\in$ D
- $\oplus$- additive operation over A.
  - Commutative and Associative
  - **0** – its unit element. a $\oplus$ **0** = a = **0** $\oplus$ a
  - Idempotent (a $\oplus$ a=a) and a $\oplus$ b=a or a $\oplus$ b=b
- $\otimes$ - multiplicative operation over A.
  - Distributive over the additive operation
  - **1** – its unit element. a $\otimes$ **1** = a = **1** $\otimes$ a
  - **0** - its annihilator: . a $\otimes$ **0** = **0** = **0** $\otimes$ a

- $a_1 \leq a_2$ iff $a_1 \oplus a_2 = a_2$
- $a_1 \oplus^{-1} a_2 = a_1$ iff $a_1 \oplus a_2 = a_2$

Security metrics as c-semirings

- Risk = $<R^+, min, +, \infty, 0>$
  - 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(a1,a2) = a2
- Trust = $<[0,1], max, \times, 0, 1>$
- Recovery time = $< R^+, min, max, \infty, 0>$

- Minimal number of attacks = $<N^+, min, +, \infty, 0>$

N-dimensional c-semirings

- N-dimensional c-semiring is a c-semiring
- $S=< \bar{D}, \oplus, \otimes, \bar{\mathbf{0}}, \bar{\mathbf{1}}>$
  - $\bar{D} =\{D^1, D^2,\ldots,D^n\}$
  - $\bar{\mathbf{0}}=\{\mathbf{0}^1, \mathbf{0}^2,\ldots,\mathbf{0}^n\}$
  - $\bar{\mathbf{1}}=\{\mathbf{1}^1, \mathbf{1}^2,\ldots,\mathbf{1}^n\}$
  - $\bar{d}_1 \otimes \bar{d}_2=(d^1_1 \otimes^1 d^1_2, d^2_1 \otimes^2 d^2_2, \ldots, d^n_1 \otimes^n d^n_2)$
  - $\bar{d}_1 \oplus \bar{d}_2 = \bar{d}_2$ iff $d^i_1 \oplus^i d^i_2 = d^i_2$ for all i;

Equational rules

- How to use history expressions to aggregate metrics:

Sequence · Parallel · choice

$$H \equiv \mathbf{1}\#H \quad \bar{d}_1\#\bar{d}_2\#H \equiv \bar{d}_2\#\bar{d}_1\#H \equiv \bar{d}_1 \otimes \bar{d}_2\#H$$

$$\bar{d}_1\#H_1 \cdot \bar{d}_2\#H_2 \equiv \bar{d}_1 \otimes \bar{d}_2\#(H_1 \cdot H_2) \quad \varphi[\bar{d}\#H] \equiv \bar{d}\#\varphi[H]$$

$$\bar{d}_1\#H_1 + \bar{d}_2\#H_2 \equiv \bar{d}_1 \oplus^{-1} \bar{d}_2\#(H_1 + H_2) \quad \bar{d}_1\#H_1 \mid \bar{d}_2\#H_2 \equiv \bar{d}_1 \otimes \bar{d}_2\#(H_1 \mid H_2)$$

$$\gamma\langle \bar{d}\#H\rangle \equiv \bar{d}'\#\gamma\langle H\rangle \quad \text{where } \gamma = T \geq_T \bar{d}'' \text{ and } \bar{d}' = \bar{d} \oplus^{-1} \bar{d}''$$

$$\mu h.H \equiv \bar{d}''\#\mu h.H' \quad \text{where } \bar{d}'' = \bigoplus_n{}^{-1}\Phi^n(\mathbf{0}) \text{ and } \Phi(\bar{d}) = \bar{d}' \Leftrightarrow \begin{cases} H[\bar{d}\#h/h] \equiv \bar{d}'\#H' \\ \wedge \\ \bar{d}'\#H' \text{ is in MNF} \end{cases}$$

loop

Example. Find a hotel

- ((40,0.93,60)#H'$_7$ + (30,0.92,90)#H'$_8$) • ((5,0.95,30)#H'$_5$ + (15,0.89,60)#H'$_6$)

- (5,0.95,30)#H'$_5$ + (15,0.89,60)#H'$_6$ = (15,0.89,60)#H'$_6$
- ((40,0.93,60)#H'$_7$ + (30,0.92,90)#H'$_8$) = undefined

- Result=((40,0.93,60)#H'$_7$ + (30,0.92,90)#H'$_8$) • (15,0.89,60)#H'$_6$

- Risk = <R^+, min, + ,∞ ,0>
- trust = <[0,1], max,×,0,1>
- Recovery time = < R^+, min, max, ∞, 0>

Abstraction. Galois insertion

- Let D^c and D^a are two sets
- Let $\subseteq$ and $\leq$ are order relations
- Galois insertion $\langle\alpha,\gamma\rangle: (D^c, \subseteq) \leftrightarrow (D^a, \leq)$
- $\alpha : D^c \rightarrow D^a$; $\gamma: D^a \rightarrow D^c$
  - α,γ monotone
  - $d^c \subseteq \gamma(\alpha(d^c))$
  - $\alpha(\gamma(d^a)) = d^a$

Order-preserving property

- D^c_1 and D^c_2 are two concrete sets
- α is order-preserving if:

$$\tilde{\bigotimes_{d\in D_1^c}} \alpha(d) \subseteq \tilde{\bigotimes_{d\in D_2^c}} \alpha(d) \Rightarrow \bigotimes_{d\in D_1^c} d \leq \bigotimes_{d\in D_2^c} d$$

Example. Find a connection

- Recovery time (order-preserving)
  - RT1 = < R^+, min, max,∞ , 0>
  - RT2 = < {vf, f, n, s, vs}, min, max, vs, vf>
  - α: [0,15] → vf; (15,50] → f; (50,100] → n; (100,300] → s; (300,∞] → vs;
  - γ: vf →15; f →50; n →100; s →300; vs → ∞;
- Trust (non order-preserving)
  - T1 = <[0,1], max,×,0,1>
  - T2 = <{1,2,3,4,5}, max,min,1,5>
  - α: [0,0.2) → 1; [0.2,0.4) → 2; [0.4,0.6) → 3; [0.6,0.8) → 4; [0.8,1) → 5;
  - γ: 5 →0.8 ; 4 →0.6; 3 →0.4; 2 →0.2; 1 → 0;

Example. Find a connection

- $((10,5,75)\#H'_1+(20,4,45)\#H'_2)\bullet($ ← Search a direct flight
  $((5,0.95,30)\#H'_5+(15,0.89,60)\#H'_6) + ($ ← Book a direct flight
  $(((5,0.98,f)\#H'_3+(8,0.95,n)\#H'_4)\bullet$ ← Search an itinerary
  $((5,0.95,30)\#H'_5+(15,0.89,60)\#H'_6)))$ ← Book an itinerary
- Recovery time is order-preserving and we can simply abstract the metric!

- $((5,0.98,f)\#H'_3+(8,0.95,n)\#H'_4 = (8,0.95,n)\#H'_4$
- $(5,0.95,30)\#H'_5+(15,0.89,60)\#H'_6 = (15,0.89,60)\#H'_6$

Different metrics Cannot be aggregated

- $(15,0.89,60)\#H'_6 \rightarrow (15,0.89,n)\#H'_6$ ← Abstract recovery time
- $(8,0.95,n)\#H'_4\bullet (15,0.89,n)\#H'_6 = (23,0.8455,n)\#H'_{11}$

Now we are able to aggregate the metric

Example. Find a connection

- $((10,5,75)\#H'_1+(20,4,45)\#H'_2)\bullet(23,0.8455,n)\#H'_{11}$
- Trust is not order preserving and we cannot simply abstract the metric
  - We align vectors of metrics by adding **1** if a metric is not in the vector
  - Continue aggregation with new vectors
  - Aggregate metrics on abstract level at the end
  - Try to make a decision
- $((10,1,5,n)\#H'_1+(20,1,4,f)\#H'_2)\bullet(23,0.8455,5,n)\#H'_{11}=$
- $=(33, 0.8455, 5, n)\#H'_{f\_1}+(43, 0.8455, 4, n)\#H'_{f\_2} =$
- $=(33, 5, n)\#H'_{f\_1}+(43, 4, n)\#H'_{f\_2} =$
- $=(43, 4, n)\#H'_{f\_2}$

Example. Find a connection

- $(43, 4, n)\#H'_{f\_2}$
- Risk: 43 < 75 satisfied
- Trust: γ(4)=0,6 < 0.8 violation
- Recovery time: γ(n)=100 < 120 satisfied

Conclusion

- We developed a unified framework analysis with security properties and metrics
  - The framework allows checking composite services in one single analysis, taking into account all alternatives
  - Any metric can be used by the method if it is specified as a c-semiring.
  - Definition of the metric as c-semiring is required once and then the metric can be used for any service
  - Few changes are required to use the framework with several metrics at ones
  - Order-preserving abstractions can easily help using different types of similar metrics
  - In same cases, we still are able to use non order-preserving abstractions making a decision at the end.