Metric-Aware Secure Service Orchestration

Gabriele Costa  
Dipartimento di Informatica, Sistemistica e Telematica  
Università di Genova  
gabriele.costa@unige.it

Fabio Martinelli  
Istituto di Informatica e Telematica  
Consiglio Nazionale delle Ricerche  
fabio.martinelli@iit.cnr.it

Artsiom Yautsiukhin  
Istituto di Informatica e Telematica  
Consiglio Nazionale delle Ricerche  
artsiom.yautsiukhin@iit.cnr.it

Secure orchestration is an important concern in the internet of service. Next to providing the required functionality the composite services must also provide a reasonable level of security in order to protect sensitive data. Thus, the orchestrator has a need to check whether the complex service is able to satisfy certain properties. Some properties are expressed with metrics for precise definition of requirements. Thus, the problem is to analyse the values of metrics for a complex business process.

In this paper we extend our previous work on analysis of secure orchestration with quantifiable properties. We show how to define, verify and enforce quantitative security requirements in one framework with other security properties. The proposed approach should help to select the most suitable service architecture and guarantee fulfilment of the declared security requirements.

1 Introduction

Orchestration of complex web services is a multidimensional problem. Various criteria must be considered when different alternatives exist. Typically, one of such criteria is security. Recently, the security issues of service composition are receiving major attention [20, 22, 4, 7, 21, 9]. Among them, formal methods have been successfully applied for modelling and analysing several different aspects of service security. In practice, these techniques generate a formal abstraction of the services under analysis. Then, a verification procedure is applied to find a formal proof of compliance between the model and the security specifications.

The first difficulty arises from service abstraction. Indeed, it is crucial that services are modelled in a “safe” way, i.e., without neglecting any security-relevant behaviour they can generate. The problem is that this feature is not always guaranteed as specification and implementation is often developed independently.

Although several, effective algorithms for software verification exist, e.g., model checking [11], they often require some modification to be applied to web services. Indeed, the algorithms typically check the compliance between a specification and a model and, if the check fails, they return a description of the detected error, e.g., a behaviour of the model that violates the specification. However, web services are designed and developed separately and they commonly have different and independent security requirements. Moreover, they are oriented to the composition and they can produce many different models, i.e., one for each possible orchestration. Hence, the verification process cannot just focus on an illegal orchestration, but should help in finding valid ones.

Service usages are often based on security metrics. Metrics conveniently use mathematical values to represent some “qualities” of a service. Several authors, e.g., see [23, 18], proposed mathematical models for the definition and composition of security metrics.

In this paper we propose an extension of previous work (see [12, 13]) on secure service orchestration integrating facilities for composing and verifying security metrics. In particular, we start from the service

*The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant numbers 257930 (ANIKETOS), 256980 (NESSOS) and 257876 (SPACIOS).
model proposed by Bartoletti et al. [4]. Roughly, they propose a type and effect system for producing safe abstractions of the behaviour of web services. Then, the authors verify these abstractions against the security policies, locally specified by each service, to find a valid composition.

We extend their model by introducing metric checks and metric annotations on their abstractions. We use a mathematical structure, called c-semiring, in order to generalise our model and be independent from the metrics used for the analysis, but still be able to reason on these metrics. Metric annotations are obtained through a new, improved type and effect system. In this way, we generate metric-annotated abstractions which contain both security and metric requirements. All the requirements are applied to different portions of the service orchestration through a local scope.

The main advantage of this approach is the possibility to model and compose both security and metric requirements in a single framework. Service developers apply security policies and metric checks to some parts of their services. Our type and effect system extracts history expressions from the implementation of the services. History expressions safely denote the behaviour of service invocations. Within a history expression, the type and effect system adds extra annotations for metrics, metric checks and security framings. Then, we adopt the same verification procedure described in [4] with special pre-processing steps for assigning correct metric labels to each service. The final result is a complete framework for defining, modelling, verifying, and enforcing both security and metric requirements in order to find valid service orchestrations.

This paper is structured as follows. Section 2 introduces the working example we will develop during our presentation. In Section 3, we describe our extension of the programming language $\lambda^{req}$ and we define its operational semantics. Then, Section 4 presents our type and effect system and Section 5 describes the analysis of security and metric requirements. Finally, Section 7 concludes the paper.

2 Running example

The travel agency BestTravel offers a travel planning service to its customers. BestTravel exploits existing services for implementing the complex task of (i) booking a connection (consisting of one or more flights) to the destination, (ii) booking a hotel room, (iii) paying the acquired items (i.e., flights and hotel room), and (iv) providing the customer with a signed receipt. As usual in service-oriented architectures, the four subtask described above are provided by existing web services.

The service developer starts from an abstract workflow describing the behaviour of BestTravel and produces a corresponding implementation. The abstract workflow depicts the atomic operations that the service must implement and how they compose each other. In the case of BestTravel, most of the atomic operations are invocations to other services. Figure 1 shows the abstract workflow of BestTravel.

![Figure 1: Abstract workflow for BestTravel.](image)

Reading Figure 1 (from left to right), we can understand the service behaviour. In words, a session of BestTravel works as follows. The service runs two procedures in parallel (rooted in $\bigtriangleup$). The first one (upper
path of the workflow) is responsible for booking a flight connection for the travel destination. In practice, BestTravel invokes a service looking for a direct flight, i.e., search direct flight. Then the execution can take two alternative branches (node): it can invoke a payment service for booking the flight, i.e., book flight, or it can start a new research for a multiple-flight connection, namely an itinerary, and book it, i.e., search itinerary and book itinerary. Concurrently, the second process (lower path) invokes services for searching and booking a hotel, i.e., search hotel and book hotel. When the two parallel procedures terminate, BestTravel iteratively invokes a digital signature service, i.e., sign line, for applying integrity and authenticity tokens to the hotel receipt and terminates.

A requirement of BestTravel is to have risk level of the performed tasks (in particular, flight booking, hotel reservation and receipt signature) less than 75. Therefore, two problems must be solved: (i) statically estimate risk for the composition plans; (2) in case some execution path in the composition plan fails the requirement, dynamically check the risk of selected paths and prevent the failure of the requirement if a risky path is selected.

### 3 Service structure

In this section we present an extended version of λ-calculus, called λ_{req}. First, we extend our previous work with two main novelties: parallel composition and metric facilities. Parallel agents in this work are defined without modifying the original syntax of the calculus. We obtain it by re-defining the operational semantics of λ_{req}. Second, we incorporate metrics into our formalism using special operations for denoting metric annotations and metric constraints. These operators are interpreted in a c-semiring mathematical structure. Metric facilities allow us to model metrics which are used in service composition.

### 3.1 Syntax

First, we define the syntax of expressions e,e′ as shown in Table 1. Briefly, * is the closed, side effects-free expression, r,r′ ∈ R denotes system resources and x,y are variables. Access events α(e),β(e′) represent the access to a certain resource, resulting from the event argument, through a specific operation/channel (e.g., α and β). Conditional term if b then e else e′ represents a branch between two expressions (where b is a boolean guard). A function is defined through the term λ x.e, where e is the function body in which x is the formal parameter and z denotes the function itself (for recursive invocations). Instead, the term e e′ denotes the application of a function e to a parameter e′. We feel free to use parenthesis for grouping either a function or its argument in order to improve readability. Security framing is used to apply the scope of a security policy ϕ to a term. We also use metric framing for expressing a term laying in the scope of a metric constraint γ. Finally, a service request req τ → τ′ denotes the invocation of a service having a certain functional interface, i.e., τ → τ′ shows that the function requires a type τ as input and produces type τ′ as output.

<table>
<thead>
<tr>
<th>e,e′ ::=</th>
<th>λ x.e  def = λ x.e with z ⊈ fv(e)</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>unit</td>
</tr>
<tr>
<td>r</td>
<td>resource</td>
</tr>
<tr>
<td>x</td>
<td>variable</td>
</tr>
<tr>
<td>α(e)</td>
<td>access event</td>
</tr>
<tr>
<td>if b then e else e′</td>
<td>branch</td>
</tr>
<tr>
<td>λ x.e</td>
<td>abstraction</td>
</tr>
<tr>
<td>e e′</td>
<td>application</td>
</tr>
<tr>
<td>ϕ[e]</td>
<td>security framing</td>
</tr>
<tr>
<td>γ(e)</td>
<td>metric framing</td>
</tr>
<tr>
<td>req τ → τ′</td>
<td>service request</td>
</tr>
</tbody>
</table>

Table 1: Syntax of λ_{req} and abbreviations
\[ \lambda x. (\text{search_flight_for}(x); \\
\quad \text{if is_available} \\
\quad \quad \text{then reserve(FLIGHT_No);FLIGHT_No} \\
\quad \quad \text{else NO_FLIGHT}) \\
\]

\[ \lambda x. (\text{generate_travel_to}(x); \text{reserve(ITINERARY);} \\
\quad \text{insurance(ITINERARY);} \text{ITINERARY}) \\
\]

\[ \lambda x. (\text{find_hotel_3s}(x); \text{book(HOTEL);} \\
\quad \text{HOTEL_RESV}) \\
\]

\[ \lambda x. (\text{if high_season} \\
\quad \text{then find_hotel_2s(x) else find_hotel_4s(x);} \\
\quad \text{book(HOTEL);HOTEL_RESV}) \\
\]

\[ \lambda x. (\text{if registered_user} \\
\quad \text{then \star else var_charge(x);buy(x);RCPT}) \\
\]

\[ \lambda x. (\text{const_charge(x);buy(x);RCPT}) \\
\]

\[ \lambda x. \text{sign_64(x);SIGN_DO} \\
\]

\[ \lambda x. \text{sign_128(x);SIGN_DO} \\
\]

**Figure 2:** Implementation of the services of Example 1

and is labelled with a unique identifier \( \rho \). Although, it is hard to create the \( \lambda^{req} \) representation for non experts such the model may be created automatically, similar to transformation of Java code [3].

For the sake of presentation, we introduce some useful abbreviations (see Table 1). Moreover, to improve the readability we feel free to use simple expressions for conditional guards, e.g., is_available or is_empty, which have a straightforward interpretation in the context we use them. We also use upper cases for resources, e.g., HOTEL and FLIGHT, and lower cases for actions, e.g., book(...) and buy(...).

According to the standard \( \lambda^{req} \) theory, we define security policies through usage automata [2]. Usage automata resemble non deterministic finite state automata (NFA) defined over the alphabet of access events. A sequence of actions is compliant with a certain policy if its corresponding usage automata does not reach a final, offending state reading the trace, i.e., valid traces are those rejected by the automata (see [2] for details).

Our main focus in this section is on the definition of metric constraints. Indeed, we introduce a syntax for defining metric checks which then we apply through metric framing. In particular a metric check has the form \( \gamma = T \geq T d \) where \( T \) is a metric name, \( \geq T \) is its order relation and \( d \) is an element of \( T \). Here we slightly abuse our notation for the sake of simplicity, in order to show that the metric computed for a business process must be better than some predefined value (i.e., threshold). In practice, a metric check is satisfied by a value \( d' \) if \( d' \geq T d \). If so we write \( d' \in \gamma \).

**Example 1.** We continue our running example. We assume the (sets of) resources: \( \mathcal{I} = \{\text{ITINERARY}\} \), \( \mathcal{F} = \{\text{FLIGHT_No, NO_FLIGHT}\} \), \( \mathcal{H} = \{\text{HOTEL_RESV}\} \), \( \mathcal{B} = \mathcal{I} \cup \mathcal{F} \cup \mathcal{H} \) and \( \mathcal{D} = \{\text{RCPT, SIGNED_DOC}\} \). In Figure 2 we propose the \( \lambda^{req} \) implementation of the services informally introduced in Section 2.

Intuitively, service 1 receives an input airport \( x \) and searches a direct flight (action search_flight_for). Then, depending on the is_available boolean flag, the service either reserves a seat (reserve) and returns the flight number FLIGHT_No, or returns the NO_FLIGHT value. Service 2 works similarly. The main difference is that, if the flight is not available, it checks whether it is possible to make an overbooking reservation (can_overbook) and proceeds with the reservation (overbook) before returning the flight number or the NO_FLIGHT value. Instead, service 3 finds a sequence of flights for the destination, namely an itinerary (generate_travel_to). Then the itinerary is reserved (reserve), a travel insurance is stipulated (insurance) and the itinerary is returned. Service 4 resembles 3, but no insurance is activated. Hotel booking services, i.e., services 5 and 6, receive a destination city \( x \) and book an hotel (action book) before returning the hotel reservation HOTEL_RESV. The main difference between the two services is that service 5 looks for a 3 stars hotel (action find_hotel_3s) while service 6, after discriminating on the flag high_season, searches either a 2 stars or a 4 stars hotel (actions find_hotel_2s and find_hotel_4s, respectively). Payment services 7 and 8 receive an item identifier \( x \) and return an electronic receipt RCPT after performing a purchase operation (action buy). However, while 8 charges the operation with a constant, extra amount (action const_charge), service
Definition 2. A c-semiring $T$ is a tuple $(D, \oplus, \otimes, 0, 1)$ where
- $D$ is a (possibly infinite) set of elements and $0, 1 \in D$;
- $\oplus$, being an addition defined over $D$, is a binary, commutative (i.e., $d_1, d_2 \in D \Rightarrow d_1 \oplus d_2 = d_2 \oplus d_1$) and associative (i.e., $d_1, d_2, d_3 \in D \Rightarrow d_1 \oplus (d_2 \oplus d_3) = (d_1 \oplus d_2) \oplus d_3$) operator such that $0$ is its unit element (i.e., $d_1 \in D \Rightarrow (d_1 \oplus 0 = d_1 = 0 \oplus d_1)$);
- $\otimes$, being a multiplication over $D$, is a binary, commutative and associative operator such that $1$ is its unit element and $0$ is its absorbing element (i.e., $d_1 \in D \Rightarrow d_1 \otimes 0 = 0 = 0 \otimes d_1$);
- $\otimes$ is distributive over additive operator $(d_1 \otimes (d_2 \oplus d_3)) = (d_1 \otimes d_2) \oplus (d_1 \otimes d_3)$;

In this work we focus on a special subset of c-semirings:

Definition 2. A c-semiring is a c-semiring with $\oplus$ satisfying the following condition: $\forall d_1, d_2 \in D \ d_1 \oplus d_2 = d_1$ or $d_1 \oplus d_2 = d_2$.
Risk, considered as possible losses, has the domain of positive real numbers. Multiplication of risks is always return the worst possible value.

\[ F(\alpha, r) = d' \]

\[ \langle \eta, d, \alpha(e) \rangle \rightarrow_\pi \langle \eta', d', \alpha(e') \rangle \]

\[ \langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle \]

\[ \langle \eta, d, \alpha(e) \rangle \rightarrow_\pi \langle \eta\alpha(r), d \otimes d', * \rangle \]

\[ \langle \eta, d, (\ell \in \mathbb{N}) \rightarrow_\pi \langle \eta', d', \ell' \rangle \]

\[ \langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle \]

In words, this operation always returns the worst possible value.

**Definition 3.** \( \leq_T \) is a total order over the set \( D \), such that \( d_1 \leq_T d_2 \) iff \( d_1 \oplus d_2 = d_2 \).

In this work we need a reverse operation for summation \( \oplus^{-1} \) which is defined as follows.

**Definition 4.** \( d_1 \oplus^{-1} d_2 = d_1 \) iff \( d_1 \oplus d_2 = d_2 \).

In words, this operation always returns the worst possible value.

**Property 1.** Operation \( \oplus^{-1} \) is associative, commutative, idempotent, distributive over \( \otimes \), and monotone.

**Example 3.** Regarding to the security targets BestTravel is going to use two metrics: trust and risk. Trust is often computed as a probability that the requested service is going to behave as agreed. Thus, trust could be seen as a value between 0 and 1, which is aggregated by multiplying and the higher value is considered better than a lower one. \( C^* \)-semiring for trust value formally is defined as follows: \( \langle [0, 1], \text{max}, \times, 0, 1 \rangle \). This type of c-semirings is known as possibilistic semiring.

Risk, considered as possible losses, has the domain of positive real numbers. Multiplication of risks is summation of possible losses, when the lower value is, naturally, considered more preferable than the higher one. Therefore, \( c^* \)-semiring for risk could be seen as \( \langle N^+ \cup \{\infty\}, \text{min}, +, \infty, 0 \rangle \), known as tropical semiring.

### 3.3 Operational Semantics

Service execution is driven by the operational semantics defined in Table 2. Intuitively, a computation step consists of a reduction from a source configuration to a target one. Configurations are tuples \( \langle \eta, d, e \rangle \) where \( \eta \) is an execution trace, i.e., the sequence of events performed so far (\( \varepsilon \) denotes the empty execution trace); \( d \) is the current metric value; and \( e \) is a \( \lambda^{req} \) term, which describes the part of the service under evaluation.

The operational semantics is driven by a composition plan \( \pi \) which is responsible for providing a mapping between each service request and an actual service, in symbols \( \pi(\rho) = \ell \) where \( \rho \) and \( \ell \) are request and service identifiers, respectively. In the following we also use \( \rightarrow_\pi^* \) for the transitive closure of \( \rightarrow_\pi \).

Below, we provide an informal explanation of the operational semantics rules. To be performed, an action \( \alpha \) requires its argument \( e \) to be evaluated first (rule \( (S-\text{Ev}_1) \)). If the action target reduces to a resource \( r \), the action takes place and the current history \( \eta \) is extended with the corresponding event \( \alpha(r) \) (rule \( (S-\text{Ev}_2) \)). Also,

\[ \langle \eta, d, \alpha(e) \rangle \rightarrow_\pi \langle \eta', d', \alpha(e') \rangle \]

\[ \langle \eta, d, (e \in \mathbb{N}) \rightarrow_\pi \langle \eta', d', e' \rangle \]

\[ \langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle \]

\[ \langle \eta, d, \alpha(e) \rangle \rightarrow_\pi \langle \eta\alpha(r), d \otimes d', * \rangle \]

\[ \langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle \]

\[ \langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle \]

\[ \langle \eta, d, \alpha(e) \rangle \rightarrow_\pi \langle \eta\alpha(r), d \otimes d', * \rangle \]

**Table 2: Operational semantics of \( \lambda^{req} \)**

**Definition 3.** \( \leq_T \) is a total order over the set \( D \), such that \( d_1 \leq_T d_2 \) iff \( d_1 \oplus d_2 = d_2 \).

In this work we need a reverse operation for summation \( \oplus^{-1} \) which is defined as follows.

**Definition 4.** \( d_1 \oplus^{-1} d_2 = d_1 \) iff \( d_1 \oplus d_2 = d_2 \).

In words, this operation always returns the worst possible value.

**Property 1.** Operation \( \oplus^{-1} \) is associative, commutative, idempotent, distributive over \( \otimes \), and monotone.

**Example 3.** Regarding to the security targets BestTravel is going to use two metrics: trust and risk. Trust is often computed as a probability that the requested service is going to behave as agreed. Thus, trust could be seen as a value between 0 and 1, which is aggregated by multiplying and the higher value is considered better than a lower one. \( C^* \)-semiring for trust value formally is defined as follows: \( \langle [0, 1], \text{max}, \times, 0, 1 \rangle \). This type of c-semirings is known as possibilistic semiring.

Risk, considered as possible losses, has the domain of positive real numbers. Multiplication of risks is summation of possible losses, when the lower value is, naturally, considered more preferable than the higher one. Therefore, \( c^* \)-semiring for risk could be seen as \( \langle N^+ \cup \{\infty\}, \text{min}, +, \infty, 0 \rangle \), known as tropical semiring.

\[ \langle \eta, d, \alpha(e) \rangle \rightarrow_\pi \langle \eta', d', \alpha(e') \rangle \]

\[ \langle \eta, d, (e \in \mathbb{N}) \rightarrow_\pi \langle \eta', d', e' \rangle \]

\[ \langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle \]

\[ \langle \eta, d, \alpha(e) \rangle \rightarrow_\pi \langle \eta\alpha(r), d \otimes d', * \rangle \]

\[ \langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle \]
the current metric is updated with the metric value for the event α(r). F is a metric and context-dependent predefined function which assigns a metric value to every event. In practice, function F can be found analytically (e.g., risk = probability × impact), derived form past experience, i.e., using monitoring or assigned by experts (e.g., number of successful virus attacks). A conditional expression is reduced to one of its branches (i.e., eť and eť×(ẽ)) depending on the value of its guard b (rule (S−If)). Here we assume an evaluation function B, assigning to each possible guard a boolean value, is to be defined. Rules (S−App1), (S−App2) and (S−App3) define the behaviour of function application. Briefly, a function e and its argument e′ are both reduced to values, i.e., terms that admit no further reduction. The steps of the two reductions are executed in a non deterministic way, without any fixed priority between the choice of (S−App1) and (S−App2). When both computations generate a value, i.e., a lambda abstraction and its argument, the application reduces to the body of the function where the formal parameter x is replaced by the actual value v and the variable z is substituted with the function itself (rule (S−App3)). Note that, along the paper, we use v, v′ to denote values, i.e., closed, effect-free terms being either *-resources, λ-abstractions or service requests. Rules (S−Sec1) and (S−Sec2) define the behaviour of the security framing. Basically, a security framing behaves as its target unless it tries to extend the current history η to an illegal trace. When the target expression reduces to a value, the policy framing can be removed, i.e., the corresponding security check is deactivated, if the current history is a legal one. Similarly, (S−Met1) and (S−Met2) rule metric checks. In words, a metric check forces metric values generated during the execution of a term e to comply with a constraint γ. Finally, service requests (rule (S−Req)) works by running the service eť with actual parameter v. Among all the compatible services, i.e., those having the same behavioural interface specified by the request p, appearing in the service repository Srť one is selected according to the current composition plan π. Note that the interface of actual services is also annotated with a history expression H which represent the service contract (see Section4 for more details on this point).

Example 4. Let eť be the implementation of service 1 proposed in Example1. We assume B(is_available) = tt, and consider the semiring Risk introduced in Example3 and the function FRisk which returns the values shown in Table3 (where missing entry evaluate to 0 and * stands for any compatible value). Then, we have the following computation for ★ = (ε,0,(eť)AIRPORT) (where AIRPORT is a resource in $^\mathcal{A}$).

<table>
<thead>
<tr>
<th>ACTION</th>
<th>RESOURCE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>reserve</td>
<td>FLIGHT_No</td>
<td>15</td>
</tr>
<tr>
<td>reserve</td>
<td>ITINERARY</td>
<td>15</td>
</tr>
<tr>
<td>overbook</td>
<td>FLIGHT_No</td>
<td>20</td>
</tr>
<tr>
<td>insurance</td>
<td>ITINERARY</td>
<td>10</td>
</tr>
<tr>
<td>find_hotel_2s</td>
<td>CITY</td>
<td>30</td>
</tr>
<tr>
<td>find_hotel_3s</td>
<td>CITY</td>
<td>20</td>
</tr>
<tr>
<td>find_hotel_4s</td>
<td>CITY</td>
<td>15</td>
</tr>
</tbody>
</table>

Table 3: Definition of function $F_{Risk}$.
In words, the computation proceeds as follows. The first step consists in applying the rule \((S\rightarrow \text{App}_3)\) which, in practice, replaces all the occurrences of \(x\) with \(\text{AIRPORT}\). The second reduction collapses two rules, i.e., \((S\rightarrow \text{Ev}_2)\) and \((S\rightarrow \text{App}_3)\). As a result of the rule \((S\rightarrow \text{Ev}_2)\) a new event, that is \(\text{search}\_\text{flight}\_\text{for}(\text{AIRPORT})\), is added to the execution trace \(\epsilon\). Also, according to the given definition of \(\mu\), the current metric is updated. Recalling the \(c^*\)-semiring specified in Example 3, we note that the multiplication operation over risk values is the sum, then \(0\otimes 0 = 0 + 0 = 0\). The subsequent step evaluates the conditional guard \(\text{is\_available}\) and chooses the “then” branch (rule \((S\rightarrow \text{If})\)). Finally, the last piece of computation repeats the operations described above and updates the current configuration by both adding a new event to the execution history and changing the current metric value (i.e., \(0\otimes 15 = 0 + 15 = 15\)). Since the term appearing in the last configuration is a value, i.e., the resource \(\text{FLIGHT\_No}\), the computation terminates.

4 Type and effect system

In this section we present our proposal for a type and effect system. It derives from the type and effect system presented in [4] from which it inherits most of its rules.

4.1 History expressions

Briefly, a type and effect system carries out the extraction of behavioural description from a certain expression while typing it. We use history expressions for representing the behaviour of a program in terms of the execution histories it can generate at runtime.

The main novelties introduced by our type and effect system are (i) parallel composition and (ii) metric annotation. Parallel composition denotes two elements which can run concurrently, in an interleaving fashion. Instead, metric annotation associate a metric value to a certain behaviour. Table 4 reports the syntax of history expressions.

A history expression can be the empty one \(\epsilon\), a variable \(h\) or an access event \(\alpha(r)\). Valid history expressions are also concatenations \((H \cdot H')\), unions \((H + H')\), parallel compositions \((H | H')\), metric-annotated expressions \((d\#H)\), security framings \((\varphi[H])\), metric checks \((\gamma(H))\) and least fix-point, recursive expressions \((\mu h.H)\).

A history expression denotes a set of execution traces. We use a denotational semantics to bind each history expression to the corresponding set of traces. The semantic function \([\cdot]\) is defined in Table 5. Note that we use the environment \(\delta\) for mapping variables to set of traces.

A \(\epsilon\) expression denotes the singleton containing the empty trace (we use \(\epsilon\) for both void history expressions and empty traces as they are clearly identified by the context). The semantics of a variable \(h\) corresponds to the set of histories associated to it in \(\delta\). A history expression \(\alpha(r)\) denotes the singleton \(\{\alpha(r)\}\). The semantics of a sequence \(H \cdot H'\) is the set of traces \(\eta\eta'\) such that \(\eta \in [H]_\delta\) and \(\eta' \in [H']_\delta\). Similarly, the semantics of a choice is the union between the sets denoted by the two sub-expressions. Parallel history expressions \(H | H'\) denote the set of all the possible interleaving of traces belonging to the two sub-expressions. Interleaving semantics is defined through the binary operator \(\cdot\). Intuitively, if one of the two considered histories is \(\epsilon\), the operator \(\cdot\) returns the other one. Instead, for non-empty traces it generates all the possible sequences representing concurrent executions. This process is obtained by considering all the possible prefixes of one trace, adding the first action of the other trace and recursively applying the \(\cdot\) operator to the remaining “tails”. In the style of [5], security framing denotes execution histories wrapped between two special actions \([\varphi]\) and \(\]_\varphi\) (for brevity, we write \(\varphi[X]\) in place of \([\varphi]\cdot X[\]_\varphi\)). These special actions mark the activation and deactivation points of a policy. Following a similar reasoning, the semantics of \(\gamma(H)\) is the set of traces denoted by \(H\) wrapped by the special

<table>
<thead>
<tr>
<th>Table 4: Syntax of history expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(H, H' := \epsilon \mid h \mid \alpha(r) \mid H \cdot H' \mid H + H' \mid H \mid H' \mid d#H \mid \varphi[H] \mid \gamma(H) \mid \mu h.H)</td>
</tr>
</tbody>
</table>
where the binary function \( \sqcup \) is recursively defined as follows.

\[
\begin{align*}
\{ \epsilon \} & = \{ \epsilon \} \\
\{ \alpha(r) \} & = \{ \alpha(r) \} \\
\{ H \cdot H' \} & = \{ H \} \sqcup \{ H' \} \\
\{ H + H' \} & = \{ H \} \cup \{ H' \} \\
\{ \phi[H] \} & = \phi\{ H \} \\
\{ d[H] \} & = \{ H \} \\
\{ \gamma[H] \} & = \gamma\{ H \} \\
\{ h \} & = \delta(h)
\end{align*}
\]

where \( \{ \cdot \} \) is the one obtained from typing the \( \cdot \) and \( \gamma \) (with the obvious meaning). Finally, \( \mu h.H \) denotes a fix point operation over the set of traces denoted by \( H \) (see \[5\] for further detail).

Moreover, we introduce a partial order relation \( \sqsubseteq \) between history expressions such that \( H \sqsubseteq H' \iff \forall \delta. \{ H \} \sqsubseteq \{ H' \} \).

### 4.2 Typing relation

In the following we introduce our typing rules. The main difference with respect to the rules proposed in previous works is that here we generate metric annotated history expressions during the typing process. Before presenting the typing rules, we need to introduce \textit{types} and \textit{type environments}.

**Definition 5.** (Types and type environments)

\[
\tau, \tau' ::= \text{unit} \mid \mathcal{R} \mid \tau \xrightarrow{H} \tau' \\
\Gamma, \Gamma' ::= \emptyset \mid \Gamma ; x : \tau
\]

A type can be both a simple type, i.e., \textit{unit} or the resource domain \( \mathcal{R} \), or a function from type \( \tau \) to type \( \tau' \). Functional types also carry a history expression \( H \) which represents the latent effect of invoking the function. Then, a type environment \( \Gamma \), being either the empty one \( \emptyset \) or the one obtained through a new binding \( \Gamma ; x : \tau \), is a mapping from variables to types.

The typing relation has the form \( \Gamma ; H \vdash e : \tau \). It must be read as “under the environment \( \Gamma \) and carrying the effect \( H \), expression \( e \) has type \( \tau \)”

The rules in Table 6 define the typing relation. 

Briefly, the expression \( * \) has \textit{unit} type and generates no side effects (\( H = \epsilon \), rule (T-Uni)) while a resource \( r \), being also side effect free, has type \( \mathcal{R} \) (rule (T-Res)). The type of a variable \( x \) depends on the typing context provided by \( \Gamma \) (rule (T-Var)). Abstractions (rule (T-Abstr)) has an empty effect and produce a functional type \( \tau \xrightarrow{H} \tau' \) from their input to their output types. The latent effect \( H \) is the one obtained from typing the function body. Rule (T-Ev) requires more attention. Indeed, we say that an expression \( \alpha(e) \), having type \textit{unit}, generates a history expression which is the sequence between the history expression deriving from typing its argument \( e \) and the summation (i.e., a finite sequence of choice operators) of all the possible access actions \( \alpha \) to a compatible resource \( r \in \mathcal{R} \). Also, all of these access events are annotated with the metric value provided by the function \( F \). The application of a function \( e \) to an argument \( e' \), i.e., rule (T-App), has type equal to the return type of \( e \) and a history effect which is the sequence between (1) the two effects of \( e \) and \( e' \) in parallel and (2) the latent effect of the function. Security and metric framing (rules (T-Frm) and (T-Met)) have the same

\[\text{Table 5: Denotational semantics}\]

---

\[\{ e \} = \{ \epsilon \} \quad \{ \alpha(r) \} = \{ \alpha(r) \} \quad \{ H \cdot H' \} = \{ H \} \sqcup \{ H' \} \quad \{ H + H' \} = \{ H \} \cup \{ H' \} \quad \{ \phi[H] \} = \phi\{ H \} \quad \{ d[H] \} = \{ H \} \quad \{ \gamma[H] \} = \gamma\{ H \} \quad \{ h \} = \delta(h)\]

\[\text{For simplicity here we assume a single set } \mathcal{R}, \text{ but, in general, we assume to have a finite number of resource domains } \mathcal{R}_1, \ldots, \mathcal{R}_n \text{ such that } \bigcup_i \mathcal{R}_i = \mathcal{R}\]
interested in a procedure which turns a history expression into a corresponding normal form. In general, it would be preferable to have a single value labelling the whole expression. In particular, we are interested in a procedure which turns a history expression into a corresponding normal form.

5.1 History expressions and semirings

Table 6: Typing relation

Example 5. Consider service 9, we call its implementation $e_9$, of Example 4. Writing it without abbreviations we obtain: $e_9 = \lambda x.(\lambda w.z.SIGNED_DOC) \text{s} \text{i} \text{g} \text{n} _{6} _{4}(x)$. Then consider the function $T_{\text{Risk}}$ of Table 3. We type $e_9$ as follows.

\[
\begin{align*}
\Gamma', \varepsilon \vdash \text{SIGNED_DOC}: \emptyset & \quad \Gamma(x) = \emptyset \\
\text{\Gamma, \varepsilon \vdash \lambda w.z: \emptyset T_{\text{Risk}} \rightarrow D} & \quad \text{\Gamma, h_0 \vdash \text{SIGN} \text{N}_6 \text{D}(x): \emptyset} \\
\emptyset, \varepsilon \vdash e_9: \emptyset T_{\text{Risk}} \rightarrow D & \quad \text{\Gamma, h_0 \vdash (\lambda w.z: \emptyset T_{\text{Risk}} \rightarrow D) \text{s} \text{i} \text{g} \text{n} _{6} _{4}(x): \emptyset}
\end{align*}
\]

where $H_0 = 1#\text{SIGN} \text{N}_6 \text{D} (\text{RCPT}) + 1#\text{SIGN} \text{N}_6 \text{D} (\text{SIGN} \text{N}_6 \text{D} \text{G} \text{O} \text{N} \text{C})$, $\Gamma = x: \emptyset T_{\text{Risk}} \rightarrow D T_{\text{Risk}} \rightarrow D$ and $\Gamma' = \gamma: za: \emptyset T_{\text{Risk}} \rightarrow D$. Following a similar reasoning we type all the services of example 4 as shown in Figure 4. For brevity, in the following we use $H_0$ to denote the latent effect of service $e_i$.

Example 6. Using the notation introduced in the previous examples for denoting the history expressions of services, we type the BestTravel implementation $e_B$ as in Figure 5. We call $H_B$ the latent effect labelling the arrow type of $e_B$.

The main result on the type and effect system is type safety. In words, type safety guarantees that effects produced by the type and effect system safely denote the behaviour of services.

\textbf{Theorem 1.} If $\Gamma, H \vdash e: \tau$ and $(\varepsilon, d, e) \rightarrow \varepsilon (\eta, d', v)$ then $\forall \delta. \eta \in [H]_{\delta}$.

Interestingly, the extensions presented in this paper do not invalidate this result originally proved by Bartoletti et al. [4]. In the next section, we show that history expressions safety is also preserved under metric factorization.

5 Security and metric analysis

5.1 History expressions and semirings

Metric annotations are used to label a history expression with metric values which are expected to be produced dynamically. However, metric annotations are locally associated with parts of a history expression while, in general, it would be preferable to have a single value labelling the whole expression. In particular, we are interested in a procedure which turns a history expression into a corresponding normal form.
For all history expressions $H$, semantics of history expressions. Such property guarantees that history expression transformations do not invalidate the equation rules of Table 7. We propose a set of equivalences that we use to move and compose metric annotations appearing in history expressions. The rules in Table 7 define the correspondence between the history expressions and the semiring operators. In particular, we can always add a multiplication-neutral annotation to a history expression.

In Table 7, we propose a set of equivalences that we use to move and compose metric annotations appearing in history expressions. The rules in Table 7 define the correspondence between the history expressions and the semiring operators. In particular, we can always add a multiplication-neutral annotation to a history expression.

A crucial property we want to prove on the equation rules of Table 7 is that they do not invalidate the metric. In Table 7, we propose a set of equivalences that we use to move and compose metric annotations appearing in history expressions. The rules in Table 7 define the correspondence between the history expressions and the semiring operators. In particular, we can always add a multiplication-neutral annotation to a history expression.

As a matter of fact, we can remove a metric check by forcing its target to be annotated with the difference between the inner annotation and the threshold of $\gamma$. Finally, a recursion is annotated with the least fix point of the function $\Phi$ that extracts the metric annotation from the inner history expression after annotating the bounded variable $h$.

A crucial property we want to prove on the equation rules of Table 7 is that they do not invalidate the semantics of history expressions. Such property guarantees that history expression transformations do not affect the safety property stated by theorem 1.

**Property 2.** For all history expressions $H$ and $H'$ if $H \equiv H'$ then $\forall \delta. [H]_\delta = [H']_\delta$
Example 7. Having in mind that $\oplus^{-1}$ is max for Risk, consider the history expression $H_2$ of Example 5:

$$H_2 = (0\#\text{search\_flight\_for}(\text{AIRPORT})) \cdot (0\#\text{reserve}(\text{FLIGHT\_No}) + 15\#\text{reserve}(\text{NO\_FLIGHT}))$$

$H_2 \equiv 0 \oplus (0 \oplus^{-1} 15)\#(\text{search\_flight\_for}(\text{AIRPORT}) \cdot (\text{reserve}(\text{FLIGHT\_No}) + \text{reserve}(\text{NO\_FLIGHT})))$

Note, that the right side of the previous equivalence is in MNF. According to the operations of the semiring Risk, the resulting annotation value is 15.

Example 8. We write the MNF of the history expressions of Example 5. For brevity, we write $H_i \equiv d_i\#H'_i$ to emphasise the metric annotation of the MNF without showing the structure of $H'_i$.

$$H_1 \equiv 20\#H'_1 \quad H_2 \equiv 15\#H'_2 \quad H_3 \equiv 25\#H'_3 \quad H_4 \equiv 15\#H'_4 \quad H_5 \equiv 40\#H'_5$$

$$H_6 \equiv 50\#H'_6 \quad H_7 \equiv 28\#H'_7 \quad H_8 \equiv 25\#H'_8 \quad H_9 \equiv 1\#H'_9 \quad H_{10} \equiv 0\#H'_{10}$$

Intuitively, Example 8 shows that every history expression appearing in our working example has an equivalent MNF. In general, we know that all the history expressions can be reduced to a corresponding MNF as stated by the following property.

Property 3. For each history expression $H$ there exists $H'$ such that $H \equiv H'$ and $H'$ is in MNF.

The last property we show is metric safety, which characterizes the most important quality of the metric annotations we generate.

Theorem 2. If $\Gamma, H \vdash e : \tau$ and $H \equiv \bar{d}\#H'$ such that $\bar{d}\#H'$ is in MNF, then for each execution $\langle \eta, d, e \rangle \xrightarrow{\gamma} \langle \eta', d', e' \rangle$ holds that $d' \leq_{\Gamma} d \otimes \bar{d}$.

Similarly to type safety, this theorem guarantees that metric annotations produced by our equational theory provide an upper bound to the metric values generated by the execution of a term. As each of them has a corresponding MNF, this theorem can be universally applied to any history expression.

5.2 Discussion

During the presentation we have shown how our formalism can be applied to the modelling of complex business processes. In this part of the article we describe how the proposed theory can be applied to the verification and analysis of the security properties of web services.

Basically, our proposal offers facilities that can be applied to all the stages of service design, implementation and execution. Statically, service designers can write their policies on execution histories and security metrics. Then, developers apply the scope of the policies to the service implementation. Finally, each service runs with proper checks controlling that the execution complies with the specification.

These steps suffice to carry out the analysis of possible configurations of a complex abstract business process. The goal is to check whether the possible configurations satisfy desired policies. This information is
required in order to decide if we can avoid run-time controls. Naturally, if a configuration satisfies a policy or the worst possible metric value is better than a threshold, there is no need for an additional control.

Note, that we assume that the declared policies/metrics for a specific service are genuine and the services are typed by a trusted type and effect system (implementation). Although this assumption is not true in general, here we focussed on the considered problem, i.e., aggregation of metrics and check of composite properties.

In order to check that a certain business process satisfies properties or has sufficiently good metric value the analyst starts for a λreq implementation of an abstract workflow, as it is shown in Example 2. Then, we assume the service repository and c∗-semirings for considered metrics to be defined similar to Examples 1 and 3. The next step is to type the service implementation similar to Example 5 and 6. Finally, we aggregate metrics annotations, as it is done in Example 7. During this process, several analysis on the validity of history expressions can be carried out in order to prevent illegal service compositions. For a description of these techniques we refer the interested reader to [4, 12].

**Example 9.** We use the history expressions in MNF shown in Example 8 to compute the MNF of $H_B$. Considering the history expression appearing in Figure 5, we can replace every instance of $H_i$ with the corresponding MNF $d_i#H'_i$. Then we obtain the following equivalences.

\[
H_B \equiv (\gamma(H_F) \cdot \gamma(H_H) \cdot \gamma(H_S))
\]

\[
H_F \equiv \left( (20#H'_1 + 15#H'_2) \cdot ((28#H'_1 + 25#H'_8) + ((25#H'_3 + 15#H'_4) \cdot (28#H'_1 + 25#H'_8)) \right)
\]

\[
H_H \equiv \left( (40#H'_5 + 50#H'_6) \cdot (28#H'_1 + 25#H'_8) \right)
\]

\[
H_S \equiv \mu h.((1#H'_6 + 0#H'_{10}) \cdot h + \epsilon)
\]

Applying the rules of Table 7 we can reduce to the following history expression.

\[
H_B \equiv (\gamma(73#H'_F) \cdot \gamma(78#H'_H) \cdot \gamma(\infty#H'_S))
\]

Recalling that $\gamma = \textbf{Risk} \leq 75$ we conclude with the equivalences below.

\[
(\gamma(73#H'_F) \cdot \gamma(78#H'_H)) \cdot (\gamma(\infty#H'_S)) \equiv (73#\gamma(H'_F) \cdot 75#\gamma(H'_H)) \cdot 75#\gamma(H'_S) \equiv 223#(\gamma(H'_F) \cdot \gamma(H'_H) \cdot \gamma(H'_S))
\]

Interestingly, we note that, among the three instances of $\gamma$, only the first one applies to a history expression satisfying the restriction, i.e., $73 \in \gamma$. We cannot say the same for the other two instances. However, our semantics for metric framing forces the execution of all the parts of the service to respect risk constraints. In this way, even though some parts of the service are labelled with $\infty$, the overall risk is a finite value, i.e., 223.

Since the last two instances fail the restriction the dynamic analysis is required. Note, that the hotel reservation part of the process may use services $H_5$ and $H_8$ with the overall risk level $65 < 75$. Therefore, during the execution we guard the second and the third instances to guarantee the low risk level values. There is no need to guard the first instance, since it satisfies the restriction in any case. Imagine, that during the execution $H_6$ service has been selected. Before executing the next step the guard must check the resulting value, using the same rules as for the static analysis. In case $H_8$ is selected the execution is allowed ($75 \leq 75$). Otherwise, if $H_7$ is chosen the restriction fails ($78 > 75$) and the execution is halted (or another action is performed, e.g., a report about the failure is sent to the customer and provider).

\[\square\]

## 6 Related work

Outsourcing processing of sensitive data to external parties requires some assurances, that the data will be well protected while processed and transmitted. Unsurprisingly, several authors claimed that security requirements must be included into the agreement between service customer and service provider [15, 16]. Our work extends the existing state of the art with a unified approach for checking security properties and security metrics of complex business processes which appear as statements in such agreements.
Many authors proposed formal languages for specifying and verifying agreements, also called contracts, between a service provider and a customer. Padovani [21] proposes a language for defining service contracts and presents a theory for the automatic generation of service orchestrators. Subcontract relations are used to find a matching between the contract offered by a service and the requirements of its clients. Similarly, Bravetti and Zavattaro [8] present a language for the specification of service contracts. Their contracts have a process algebra-based semantics and allow for the specification of composed services. Contract composition can be verified to guarantee that the interaction of a group of services does not violate the specifications. Even though these works do not focus on security analysis, their contracts can be adapted to model security requirements.

Martinelli and Matteucci [17] presented a framework for the synthesis of a secure orchestrator, i.e., an agent which drives the interaction between two services guaranteeing that a certain security policy is respected. Although, the proposals described above use contracts for the specification and analysis of history-based [11] service properties, none of them allows for the definition of security metrics and restrictions on them.

In order to check whether a complex business process satisfies some quantitative requirements aggregation of security metric values for atomic services is required. For example, Cheng et. al. [10] aggregated downtime metric, considering business process like a simple set of activities, i.e., regardless the operational flow.

In contrast, Jaeger et. al. [19] have shown that some metrics could be aggregated differently depending on the structural activity used for joining the atomic services. In this work all metrics were considered separately. Moreover, the author did not considered security metrics. Yu et. al. [24, 23] applied the idea of Jeager at. al. for selection of the best process among several alternatives. The authors defined aggregation functions for several metrics and aimed at selection of the best alternative which satisfies the constraints specified in the agreement. First the authors defined a utility function and proposed to solve a 0-1 multi-dimension multi-choice knapsack problem (MMKP) only for a sequential order [23]. Solutions for a general workflow were proposed later [24].

Massacci and Yautsiukhin [18] proposed a method and an algorithm for aggregation of security metrics. The authors also solved the problem of selection the best (i.e., more secure) alternative, though a wider range of metrics were considered (these metrics cannot be used in classical algorithms for finding the shortest path). The method was extended for checking several metrics at the same time using Pareto optimality strategy [14].

In our work we do not have a goal to select the business process which has the best metric value. Moreover, we assume that some processes which do have a value worse than desired may still satisfy the policy if a more secure execution path is selected for a specific invocation. Therefore, our proposal allows making a decision at design time and supporting control at run-time.

### 7 Conclusion

In this paper we presented a novel approach for dealing with the analysis and verification of both security and metric requirements of web services. Our system is developed on existing solutions for modelling security and metric-based requirements. The result is a unified framework for (i) the definition and application of security and metric policies within service implementation, (ii) the automatic extraction of history expressions carrying metric annotations and (iii) the computation (through an equational theory) of metric values which safely predict the expected behaviour of services. Our proposal requested a new type and effect system, extending existing approaches, to be defined. Interestingly, we found that adding metric annotations does not invalidate the type safety property, i.e., annotations are orthogonal to the history expressions.

The present work is a first step toward a complete model for the specification and verification of quantitative and qualitative, non functional requirements for web services. Further effort is requested in order to generalise our approach. In particular, we aim at defining a procedure for generating orchestration plans starting from the history expressions produced by our type and effect system. Such method has been presented in [4] for metric-free history expressions and we believe that similar results can be extended to our proposal. Another limitation of the current model is our static description of metric value for the events. Even though we think that assigning metric values to events is a reasonable way to model the actual behaviour of services, it is not always correct to assume these values to keep unchanged in time. Indeed, many metrics aim at modelling dynamic evolution of some property, e.g., reputation or number of system failures, which we cannot model with our approach.
References


Proofs

Property 1. Operation $\oplus^{-1}$ is associative, commutative, idempotent, distributive over $\otimes$, and monotone

Proof. Commutative. We must prove that $d_1 \oplus^{-1} d_2 = d_1 \oplus^{-1} d_2$. Let $d_1 \oplus^{-1} d_2 = d_2$, then $d_1 \oplus d_2 = d_1$. Since $\oplus$ is commutative, then $d_2 \oplus d_1 = d_1$. This means that $d_2 \oplus^{-1} d_1 = d_2 = d_1 \oplus^{-1} d_2$. Using the same reasoning we can prove the same property for $d_1 \oplus^{-1} d_2 = d_1$.

Associative. We must prove that $d_1 \oplus^{-1} (d_2 \oplus^{-1} d_3) = (d_1 \oplus^{-1} d_2) \oplus^{-1} d_3$. Let $d_2 \leq d_3$ and $d_2 \oplus^{-1} d_3 = d_2$. Thus $d_1 \oplus^{-1} (d_2 \oplus^{-1} d_3) = d_1 \oplus^{-1} d_2$. Note, that $d_1 \oplus^{-1} d_2 \leq d_2 \leq d_3$ and we can add $d_3$ without changing the result: $d_1 \oplus^{-1} (d_2 \oplus^{-1} d_3) = (d_1 \oplus^{-1} d_2) \oplus^{-1} d_3$. The same can be proven for $d_3 \leq d_2$.

Distributive over $\otimes$. We must prove that $d_1 \otimes (d_2 \oplus^{-1} d_3) = (d_1 \otimes d_2) \oplus^{-1} (d_1 \otimes d_3)$. Lets $d_2 \leq_T d_3$. This means that $d_2 \oplus^{-1} d_3 = d_2$ and $d_2 \oplus d_3 = d_3$. From distribution property of summation we know that $(d_1 \otimes d_2) \oplus (d_1 \otimes d_3) = d_1 \otimes (d_2 \oplus d_3) = d_1 \otimes d_2$. This means that $(d_1 \otimes d_2) \oplus^{-1} (d_1 \otimes d_3) = d_1 \otimes d_3 = d_1 \otimes (d_2 \oplus^{-1} d_3)$. Using the same reasoning we can prove the same property for $d_3 \leq_T d_2$.

Idempotent. We must prove that $d_1 \oplus^{-1} d_1 = d_1$. Let $d_1 = d_2$. Then, $d_1 \oplus d_2 = d_1 = d_2$. Thus, $d_1 \oplus^{-1} d_2 = d_1 \oplus^{-1} d_1 = d_1$.

Monotone. We must prove that if $d_1 \leq d_2$ then $\forall d_3 d_1 \oplus^{-1} d_3 \leq d_2 \oplus^{-1} d_3$. Since $d_1 \leq d_2$ then if $d_1 \oplus^{-1} d_2 = d_1$ and $d_1 \oplus^{-1} d_2 \oplus^{-1} d_3 = d_1 \oplus^{-1} d_3$. By idempotence of $\oplus^{-1}$: $d_1 \oplus^{-1} d_3 = d_1 \oplus^{-1} d_2 \oplus^{-1} d_3 = d_1 \oplus^{-1} d_2 \oplus^{-1} d_3 \leq d_2 \oplus^{-1} d_3$. The last part implies that $d_1 \oplus^{-1} d_3 \leq d_2 \oplus^{-1} d_3$.

Lemma 1. Let $\Gamma, \mathcal{H} \vdash e : \tau$ and $\langle \eta, d, e \rangle \rightarrow_\pi \langle \eta', d', e' \rangle$. If $\Gamma, \mathcal{H}' \vdash e' : \tau$ then $\forall \delta. \eta'[\mathcal{H}']_\delta \subseteq \eta[\mathcal{H}]_\delta$

Proof. By induction on the depth of $\Gamma, \mathcal{H} \vdash e : \tau$.

- Case (T–Unit), (T–Res) and (T–Var). Trivial.
- Case (T–Ev). We have two further cases
  a) $\langle \eta, d, \alpha(\bar{e}) \rangle \rightarrow_\pi \langle \eta', d', \alpha(\bar{e}') \rangle$, then we instantiate the hypothesis to

  \[
  \begin{array}{l}
  \Gamma, \mathcal{H} \vdash \bar{e} : \mathcal{R} \\
  \hline
  \Gamma, \mathcal{H} : \sum_{\alpha} F(\alpha, r) \# \alpha(r) \vdash \alpha(\bar{e}) : unit
  \end{array}
  \]

  and

  \[
  \begin{array}{l}
  \langle \eta, d, \bar{e} \rangle \rightarrow_\pi \langle \eta', d', \bar{e}' \rangle \\
  \hline
  \langle \eta, d, \alpha(\bar{e}) \rangle \rightarrow_\pi \langle \eta', d', \alpha(\bar{e}') \rangle
  \end{array}
  \]

  Assuming the premises of the two rules and applying the inductive hypothesis we infer that $\Gamma, \mathcal{H}' \vdash \bar{e}' : \mathcal{R}$ implies that $\forall \delta. \eta'[\mathcal{H}']_\delta \subseteq \eta[\mathcal{H}]_\delta$. Applying the typing rule for events we have

  \[
  \begin{array}{l}
  \Gamma, \mathcal{H}' \vdash \bar{e}' : \mathcal{R} \\
  \hline
  \Gamma, \mathcal{H}' : \sum_{\alpha} F(\alpha, r) \# \alpha(r) \vdash \bar{e}' : \mathcal{R}
  \end{array}
  \]

  Then $\forall \delta. \eta'[\mathcal{H}']_\delta \subseteq \eta[\mathcal{H}]_\delta \subseteq \eta[\sum_{\alpha} F(\alpha, r) \# \alpha(r)]_\delta$.

  b) $\langle \eta, d, \alpha(r) \rangle \rightarrow_\pi \langle \eta \alpha(r), d \otimes F(\alpha, r) \rangle$. We assume the premise

  \[
  \begin{array}{l}
  \Gamma, e \vdash r : \mathcal{R} \\
  \hline
  \Gamma, \sum_{\alpha} F(\alpha, r) \# \alpha(r) \vdash \alpha(r) : unit
  \end{array}
  \]

  and we simply note that $\forall \delta. \eta \alpha(r)[e]_\delta \subseteq \eta[\sum_{\alpha} F(\alpha, r) \# \alpha(r)]_\delta$. 
• Case (T→If). We have two symmetric cases (depending on $\mathcal{B}(b)$). Instantiating the rule we obtain
\[
\Gamma, H \vdash e_\eta : \tau \quad \Gamma, H \vdash e_{\eta} : \tau
\]
and
\[
\langle \eta, d, \text{if } b \text{ then } e_\eta \text{ else } e_\eta \rangle \rightarrow_{\pi} \langle \eta_\eta, d, e_\mathcal{B}(b) \rangle
\]
By inductive hypothesis we have that $\forall \delta$ the property holds on both $e_\eta$ and $e_{\eta}$, which suffices to conclude.

• Cases (T→Abs) and (T→Req). Premises are false, then the property holds.

• Case (T→Fzm). Instantiating the premises we have
\[
\Gamma, H \vdash e : \tau
\]
and
\[
\langle \eta, d, e \rangle \rightarrow_{\pi} \langle \eta', d', e' \rangle \quad \eta' \models \varphi
\]
Then, applying the inductive hypothesis we obtain that $\Gamma, H' \vdash e' : \tau$ implies that $\forall \delta. \eta'([H'])_\delta \subseteq \eta([H])_\delta$.

Here we must prove that $\forall \delta. \eta'([\varphi[H']])_\delta \subseteq \eta([\varphi[H]])_\delta$. To do that, we make explicit the two sets
\[
A = \eta'([\varphi[H']])_\delta = \{ \eta' \eta' | \eta' \models \varphi \land \exists \eta' \in [H']_\delta. \eta' \leq \eta' \}
\]
\[
B = \eta([\varphi[H]])_\delta = \{ \eta \eta | \eta \models \varphi \land \exists \eta \in [H]_\delta. \eta \leq \eta \}
\]
and we prove that $\bar{\eta} \in A \Rightarrow \bar{\eta} \in B$. From the definition of $A$ we know that $\bar{\eta} = \eta' \eta'$. Then, there must be $\bar{\eta}' \in [H']_\delta$ extending $\eta'$. By inductive hypothesis $\eta' \eta' \in \eta'([H'])_\delta$ implies that $\eta' \eta' \in \eta([H])_\delta$.

As $\eta' = \eta \bar{\eta}$ for some $\bar{\eta}$ (execution can only extend traces), $\eta \eta' \in [H]_\delta$. Since $\eta \eta'$ complies with $\varphi$ and it is a sub-trace of a history $(\eta \eta')$ in $[H]_\delta$ there must be $\eta \eta' \eta' \in B$. The thesis follows from $\eta \eta' \eta' = \eta' \eta' = \eta$.

• Case (T→Met). We follow the same reasoning of the previous case.

• Case (T→App). Let $e = e_1 e_2$. We have
\[
\Gamma, H_0 \vdash e_1 : \tau \quad H_2 \quad \Gamma, H_1 \vdash e_2 : \tau
\]
We must verify three possible subcases depending on the rule used to derive $\langle \eta, d, e_1 e_2 \rangle$.

- If (S→App) is used, then
\[
\langle \eta, d, e_1 \rangle \rightarrow_{\pi} \langle \eta', d', e'_1 \rangle
\]
Applying the inductive hypothesis to $e_1$ we infer that the property holds on $\Gamma, H \vdash e'_1 : \tau \rightarrow_{H_2} \tau'$. Then, we apply (T-App) and we have
\[
\Gamma, H \vdash e'_1 : \tau \quad H_2 \quad \Gamma, H_1 \vdash e_2 : \tau
\]

\[
\Gamma, (H_0 \mid H_1) \cdot H_2 \vdash e_1 e_2 : \tau'
\]
Lemma 2. Let $x \in f v(e)$ then for all $\Gamma, e', \tau, \tau'$

$$\Gamma[\{e'/x\}], H \vdash e : \tau \land \Gamma, H' \vdash e' : \tau' \implies \Gamma, H'' \vdash e\{e'/x\} : \tau$$

for some $H, H'$ and $H''$.

Proof. By induction over $e$ we have

- $e = *$, $e = r$, $e = \tau \in \mathcal{Q}_\rho \tau_1 \rightarrow \tau_2$. Trivial.
- $e = x$. Here $e\{e'/x\} = e'$ and the property is trivially satisfied because $\tau = \tau'$.
- All the other cases are satisfied by the inductive hypothesis (just note that for conditional we also need to apply the weakening rule).

Lemma 3. If $\Gamma, H \vdash e : \tau$ and $\langle \eta, d, e \rangle \rightarrow^*_{\pi} \langle \eta', d', e' \rangle$ then $\exists H'$ such that $\Gamma, H' \vdash e' : \tau$

Proof. We prove this lemma in two steps. We first prove that (1) the property holds for one step reductions and then (2) we prove it on arbitrary long reductions.

1. If $\Gamma, H \vdash e : \tau$ and $\langle \eta, d, e \rangle \rightarrow^*_{\pi} \langle \eta', d', e' \rangle$ then $\exists H'$ such that $\Gamma, H' \vdash e' : \tau$. By induction over $e$.

   - $e = *$, $e = r$, $e = x$, $e = \lambda x. e'$, $e = \tau \in \mathcal{Q}_\rho \tau_1 \rightarrow \tau_2$. Trivial.
• \( e = \alpha(e') \). By \((T-Ev)\) we have

\[
\Gamma, H \vdash e' : R
\]

\[
\Gamma, H \cdot \sum_{r \in R} (F(\alpha, r) \# \alpha(r)) \vdash \alpha(e) : \text{unit}
\]

Hence \( e \) can make a transition either according to \((S-Ev_1)\) or \((S-Ev_2)\). In the first case we have

\[
\langle \eta, d, e' \rangle \rightarrow_\pi \langle \eta', d', e'' \rangle
\]

Applying the inductive hypothesis to \( e'' \) we know that there exists \( H'' \) s.t. \( \Gamma, H'' \vdash e'' : R \) hence we conclude by applying \((T-Ev)\). Instead, in the second case, we obtain

\[
F(\alpha, r) = d'
\]

\[
\langle \eta, d, \alpha(r) \rangle \rightarrow_\pi \langle \eta, \alpha(r), d \otimes d', * \rangle
\]

and the property is trivially satisfied with \( \Gamma, e \vdash * : \text{unit} \).

• \( e = \text{if } b \text{ then } e_1 \text{ else } e_2 \). Here we have two symmetric cases depending on the evaluation of \( b \). By the inductive hypothesis the property holds on both \( e_1 \) and \( e_2 \). However, for \((S-\text{If})\), \( e \) reduces to either \( e_1 \) or \( e_2 \), which suffices to conclude.

• \( e = e_1 e_2 \). By \((T-\text{App})\) here we have

\[
\Gamma, H_1 \vdash e_1 : \tau_2 \quad \Gamma, H_2 \vdash e_2 : \tau_2
\]

\[
\Gamma, (H_1 \cdot H_2) \vdash e_1 e_2 : \tau
\]

In this case there are three possible rules: \((S-\text{App}_1)\), \((S-\text{App}_2)\) or \((S-\text{App}_3)\). The first two are similar and we solve them at once. Indeed, we just need to apply the inductive hypothesis to the right hand side expression \( e_1' \) (\( e_2' \), respectively) and we can use the typing rule \((T-\text{App})\) to conclude. In the third case we have \( e_1 = \lambda\alpha. e' \) and \( e_2 = v \), then we instantiate \( \alpha \) and \( \text{App} \) to concluding

\[
\langle \eta, d, (\lambda\alpha. e')v \rangle \rightarrow_\pi \langle \eta, d, e' \{v/x, \lambda\alpha. e' / z\} \rangle
\]

We can conclude by applying lemma 2 to \( e' \).

• \( e = \varphi[e'] \), \( e = \gamma(e') \). Trivially by applying the inductive hypothesis to \( e' \)

2. By induction on the length of the derivations. The base case is satisfied by the property at point (1). Then, the inductive step, simply consists of applying (1) to the inductive hypothesis.

\[\square\]

**Lemma 4.** If \( \Gamma, H \vdash e : \tau \) then there exists \( \tilde{H} \) such that \( \Gamma, \tilde{H} \vdash e : \tau \) and \( \forall H''. \Gamma, H'' \vdash e : \tau \Rightarrow \tilde{H} \subseteq H'' \).

**Proof.** By induction on the depth of \( \Gamma, H \vdash e : \tau \).

• Case \((T-\text{Unit})\), \((T-\text{Res})\), \((T-\text{Var})\), \((T-\text{Abs})\) and \((T-\text{Req})\). Trivially \( \tilde{H} = \varepsilon \).

• Case \((T-\text{Wkn})\). Trivial, by the inductive hypothesis.

• Case \((T-Ev)\). We have

\[
\Gamma, H \vdash e : R
\]

\[
\Gamma, H \cdot \sum_{R} F(\alpha, r) \# \alpha(r) \vdash \alpha(\tilde{e}) : \text{unit}
\]
By applying the inductive hypothesis to $\bar{e}$, we find $\bar{H}_e$. Hence, we just need to notice that $\bar{H}_e \cdot \sum_\Delta F(\alpha, r) \# \alpha(r)$ is the minimal history expression typing $e$ (the summation factor cannot be modified/removed by any other rule).

- Case $(\text{T-If})$. We have

$$\Gamma, H \vdash e : \tau \quad \Gamma, H \vdash e_f : \tau$$

$$\Gamma, H \vdash \text{if } b \text{ then } e_u \text{ else } e_f : \tau$$

By inductive hypothesis, there exist $\bar{H}_0$ and $\bar{H}_f$. We show by contradiction that $\bar{H} = \bar{H}_0 + \bar{H}_f$. Assume there exists $\bar{H}' \subseteq \bar{H}$ such that $\Gamma, H' \vdash \text{if } b \text{ then } e_u \text{ else } e_f : \tau$. By $(\text{T-If})$, we have that $\bar{H}_0 \subseteq \bar{H}'$ and $\bar{H}_f \subseteq \bar{H}'$. However, this implies that $\bar{H} \subseteq \bar{H}' \bar{H}$ which suffices to conclude.

- Cases $(\text{T-Frm})$ and $(\text{T-Met})$. Direct consequence of the inductive hypothesis.
- Case $(\text{T-App})$. We have

$$\Gamma, H_0 \vdash e_1 : \tau \quad \delta_1 \Gamma, H_1 \vdash e_2 : \tau$$

$$\Gamma, (H_0 \mid H_1) \cdot H_2 \vdash e_1 e_2 : \tau'$$

Applying the inductive hypothesis we find $\bar{H}_0, \bar{H}_1$ and $\bar{H}_2$ and we show that $\bar{H} = (\bar{H}_0 \mid \bar{H}_1) \cdot \bar{H}_2$. By contradiction, let assume that there exists $\bar{H}' \subseteq \bar{H}$. By rule, $(\text{T-App})$ we have that $\bar{H}' = (\bar{H}_0' \mid \bar{H}_1') \cdot \bar{H}_2'$ such that $\bar{H}_i \subseteq H_i'$ (with $i \in \{0, 1, 2\}$). However, this implies $\bar{H} = (\bar{H}_0 \mid \bar{H}_1) \cdot \bar{H}_2 \subseteq (\bar{H}_0' \mid \bar{H}_1') \cdot \bar{H}_2' = \bar{H}' \subseteq \bar{H}$.

**Lemma 5. (Subject reduction)** Let $\Gamma, H \vdash e : \tau$ and $\langle \eta, d, e \rangle \rightarrow^* \pi \langle \eta', d', e' \rangle$. If $\Gamma, H' \vdash e' : \tau$ and $\forall H''. \Gamma, H'' \vdash e' : \tau \Rightarrow H' \subseteq H''$ (i.e., $H'$ is the minimal history expression typing $e'$) then $\forall \delta. \eta^\pi H''_\delta \subseteq \eta H_\delta$.

**Proof.** Then, we proceed by induction on the length of the derivations.

- Base case. In this case $e = e'$ and $\eta = \eta'$. By lemma 4 there exists $\bar{H}$ which satisfies the property.
- Inductive step. Here we have $\langle \eta, d, e \rangle \rightarrow^* \pi \langle \eta', d', e' \rangle \rightarrow^\pi \langle \eta'', d'', e'' \rangle$. We apply the inductive hypothesis to the first part of the derivation. Then we need to apply lemma 1 to $\langle \eta', d', e' \rangle \rightarrow^\pi \langle \eta'', d'', e'' \rangle$. For doing that, we have to be sure that there exists $H''$ such that $\Gamma, H'' \vdash e'' : \tau$, which is guaranteed by lemma [3]. We conclude by applying lemma 1 to $H''$ and we find $H''$ minimal.

**Theorem 1.** If $\Gamma, H \vdash e : \tau$ and $\langle \varepsilon, d, e \rangle \rightarrow^* \pi \langle \eta', d', v \rangle$ then $\forall \delta. \eta \in [H]_\delta$.

**Proof.** Theorem 1 is just a corollary of lemma 5 in the particular case in which $e' = v$, $\eta' = \varepsilon$ and $H' = \varepsilon$.

**Property 2.** For all history expressions $H$ and $H'$ if $H \equiv H'$ then $\forall \delta. [H]_\delta = [H']_\delta$

**Proof.** We proceed by induction on the equational rules. Most cases are trivially implied by the history expressions semantics defined in Table 5. Here we just show the cases requiring some more explanations.

- Case $d_1 \# H_1 \cdot d_2 \# H_2 \equiv d_1 \otimes d_2 \# (H_1 \cdot H_2)$. By inductive hypothesis and semantics of annotated history expressions we have

$$[[d_1 \# H_1 \cdot d_2 \# H_2]]_\delta = [[H_1 \cdot H_2]]_\delta = [[d_1 \otimes d_2 \# (H_1 \cdot H_2)]]_\delta$$

- Case $d_1 \# H_1 + d_2 \# H_2 \equiv d_1 \oplus^{-1} d_2 \# (H_1 + H_2)$. Following the same reasoning of the previous case

$$[[d_1 \# H_1 + d_2 \# H_2]]_\delta = [[H_1 + H_2]]_\delta$$

$$= [[d_1 \oplus^{-1} d_2 \# (H_1 + H_2)]]_\delta$$
Proof. We proceed by induction over $\eta$, $\varepsilon$, $h$, and $\alpha(r)$. Trivial.

- Case $H_1 \cdot H_2$. We apply the inductive hypothesis and we find the MNFs $d_1 \#H_1'$ and $d_2 \#H_2'$. By the rules of Table 7, $d_1 \otimes d_2 \#H_1' \cdot H_2' \equiv d_1 \#H_1' \cdot d_2 \#H_2'$ is a MNF for $H$.

- Case $H_1 + H_2$ and $H_1 | H_2$. We follow a reasoning analogous to the previous case.

- Case $d \#H$. By the inductive hypothesis we know there exists a MNF $d' \#H'$ for $H$. We conclude by noticing that $d \otimes d' \#H'$ is a MNF for $d \#H$.

- Case $\varphi[H]$. A direct consequence of the inductive hypothesis.

- Case $\gamma\langle H \rangle$. A consequence of the inductive hypothesis and the equivalence rule for metric checks.

- Case $\mu h. H$. By inductive hypothesis $H$ has a corresponding MNF $d' \#H'$. Then, we apply the equivalence rule and we find $\mu h. H \equiv d' \#\mu h. H'$ (for some $d$) which is in MNF.

Property 3. For each history expression $H$ there exists $H'$ such that $H \equiv H'$ and $H'$ is in metric normal form.

Theorem 2. If $\Gamma, H \vdash e : \tau$ and $H \equiv d' \#H'$ such that $d' \#H'$ is in MNF, then for each execution $\langle \eta, d, e \rangle \rightarrow^*_{\pi} \langle \eta', d', e' \rangle$ holds that $d' \leq_{T} d \otimes d'$.

Proof. We first prove that the property holds for single-step computations (by induction on $e$) and then we prove the theorem by induction on the length of the computations.

- Cases $\ast$, $r$ and $x$. Trivial.

- Case $\alpha(e)$. Here we have two possibilities. If $(S-Ev_1)$ applies, the property is guaranteed by the inductive hypothesis. Instead, if $(S-Ev_2)$ is used then $e = r$ and we have that $d' = d \otimes F(\alpha, r)$. However, the MNF of the history expression returned by the type system is $\bigoplus_{T}^{-1} F(\alpha, r) \# \cdots$ which trivially satisfies the property.

- Case $\textbf{if} b \textbf{then} e \textbf{else} e'$. Here the computation reduces to one between $e$ and $e'$. However, the MNF for it is always annotated with $d_1 \oplus^{-1} d_2$, which respectively annotate the MNFs for $e$ and $e'$, and the property holds.

- Cases $\lambda x.e$ and $\text{req}_p \tau \rightarrow \tau'$. Hypothesis does not apply.

- Case $e e'$. Here the MNF is $d_1 \otimes d_2 \otimes d_3$, which annotate the MNF for $e$, $e'$ and the latent effect of $e$, respectively. Independently of the rule we apply, i.e., $(S-App_1)$, $(S-App_2)$ or $(S-App_3)$, we always reduce to the inductive hypothesis.

- Case $\varphi[e']$. By inductive hypothesis.

- Case $\gamma(e')$. Assuming $\gamma = T \leq_{T} d$, by hypothesis, the term allows one computation steps, that is, it does not violate $\gamma$. Hence, $d' \leq d \oplus^{-1} d$ which labels the MNF for the history expression of $e$.

We complete by induction on the derivation length.
• Base case (zero-step computations). Trivially \( d' = d \).

• Induction. We have

\[
\langle \eta, d, e \rangle \xrightarrow{\pi} \langle \eta', d', e' \rangle \xrightarrow{\pi} \langle \eta'', d'', e'' \rangle
\]

By the inductive hypothesis we know that \( d' \leq_T d \otimes \bar{d} \) and we proceed by co-induction on the rules of the operational semantics.

- Cases \((S-\text{If}), (S-\text{App_3}), (S-\text{Sec_2}), (S-\text{Met_2})\) and \((S-\text{Req})\). Trivial as \( d'' = d' \).

- Cases \((S-\text{Ev_1}), (S-\text{App_1}), (S-\text{App_2}), (S-\text{Sec_1})\) and \((S-\text{Met_1})\). Trivially reduce to the inductive hypothesis.

- Case \((S-\text{Ev_2})\). Here \( d'' = d' \otimes F(\alpha, r) \). However, as \( \alpha(r) \) is typed according to rule \((T-\text{Ev})\), we have \( d' \otimes F(\alpha, r) \leq_T d' \otimes \oplus_{r'}^{-1} F(\alpha, r') = d' \oplus_{r'}^{-1} F(\alpha, r') \oplus_{-1} F(\alpha, r) \) (for each specific \( r \), according to the definition of \( \oplus_{-1} \)). But then we have \( d \geq_T d' \oplus_{-1} F(\alpha, r) \) which suffices to conclude.

\[\blacksquare\]