


THE **ATMOSPHERE** APPROACH FOR TRUSTWORTHY CLOUD SERVICES

POSEIDON Workshop
Coimbra, Portugal
July 10th, 2019

Marco Vieira
mvieira@dei.uc.pt
Department of Informatics Engineering
University of Coimbra - Portugal



ATMOSPHERE

Adaptive, Trustworthy, Manageable, Orchestrated, Secure, Privacy-assuring, Hybrid Ecosystem for REsilient Cloud Computing

- Ongoing EU/Brazil H2020 project
- Provide a solution to enable the implementation of trustworthy and resilient cloud services
 - On top of an intercontinental hybrid and federated resource pool
- Broad spectrum of trustworthiness properties
 - Strong focus on security and privacy

Marco Vieira POSEIDON, July 10th, 2019, Coimbra, Portugal 2

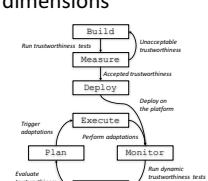
CONSORTIUM



Marco Vieira POSEIDON, July 10th, 2019, Coimbra, Portugal 3

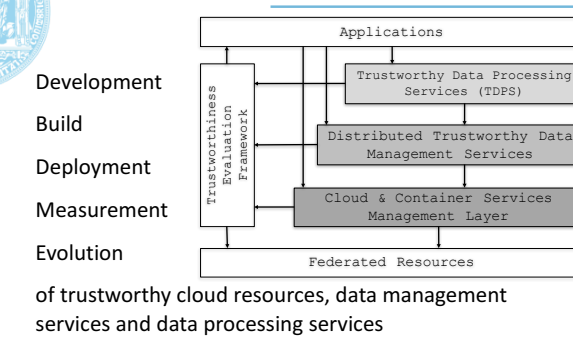
TRUSTWORTHINESS LIFE-CYCLE

- Trustworthiness is considered in multiple dimensions
 - Security, Privacy, Coherence, Isolation, Stability, Fairness, Transparency and Dependability
- Trustworthiness scores define the properties that can be evaluated in each one of these dimensions
 - A priori and a posteriori evaluation
 - Enabling self-adaptive applications
 - Tracing the degree of compliance with regulations such as the GDPR
 - Privacy protection, traceability, confidentiality warning, etc.



Marco Vieira POSEIDON, July 10th, 2019, Coimbra, Portugal 4

TRUSTWORTHINESS FRAMEWORK...



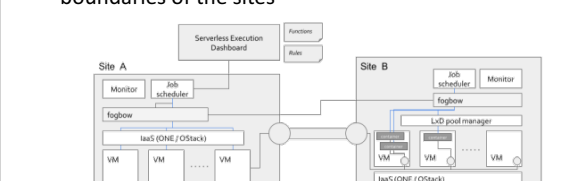
Development
Build
Deployment
Measurement
Evolution

of trustworthy cloud resources, data management services and data processing services

Marco Vieira POSEIDON, July 10th, 2019, Coimbra, Portugal 5

HYBRID FEDERATED CONTAINER PLATFORM

- A hybrid and federated platform for trustworthiness
- VMs and Docker containers as first class hypervisors
- Federated network management beyond the boundaries of the sites

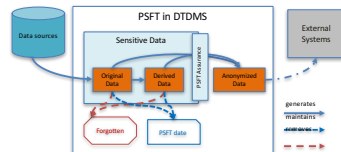


Marco Vieira POSEIDON, July 10th, 2019, Coimbra, Portugal 6

TRUSTWORTHY DATA MANAGEMENT SERVICES

Support storage, retrieval, update and access to data
— Guaranteeing confidentiality, revocation, access control, ...

- Policy engines for Secure Data Management
- Based on enclaves and focusing on SQL and NoSQL DBs
- Privacy preservation and annotation



Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

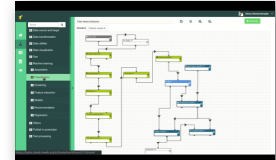
7

TRUSTWORTHY DATA PROCESSING SERVICES

Layer of data analytic techniques implemented as a set of building blocks

— As well as a framework for the development of applications from the building blocks on top of the platform

- Evaluation of privacy risks, estimation of execution deadlines for a given resource allocation
- Workflow orchestration



Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

8

EXPECTED OUTPUTS

- A definition of trustworthiness properties
- A platform to characterize such properties
- A hybrid and federated container-based infrastructure
- Performance modelling services for the applications
- Trustworthy Data Management and Processing services
- A use case on telemedicine - processing of *echocardio* images

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

9

TRUSTWORTHINESS PROPERTIES

Trust. Prop.	Explanation
Security	Covering Integrity, Availability, Confidentiality, we define it as the attack resistance and fault tolerance against malicious attacks.
Privacy assur.	Guarantee of an entity to be secure from unauthorized disclosure of sensible info.
Coherence	Consistency of the information regardless of the location.
Isolation	The effects of a service do not impact the trustworthiness of other data & services (e.g. crashes, starvation or privacy issues of a service do not compromise others).
Stability	The service produces equivalent outcomes and QoS for equivalent inputs and resources used.
Fairness	The assurance of ethical and legal rights.
Transparency	Involves multiple sub-dimensions, such as Awareness, Access, Redress (capability of rectifying), Explanation, Provenance, Auditability and Accountability (assign responsibility to services and their outcomes).
Dependability	Includes multiple sub-dimensions, such as Integrity (absence of improper system alterations), Availability (readiness for correct service), Reliability (continuity of correct service), Maintainability (ability to undergo modifications and repairs), Safety (absence of catastrophic consequences on the user(s) and the environment), and Performance stability over time.

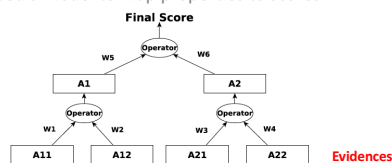
Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

10

FROM PROPERTIES TO SCORES...

A property may require several different scores
— We need a model to map properties to scores



- Calculating a score requires collecting raw data
— Trust evolves over time...
- Coherence vs Stability vs Fairness vs ...

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

11

TWO PHASES...

Design-time assessment

- Assure specific properties before deployment
- Development -> Assessment -> Development cycle until expected level of trustworthiness is achieved
- Measurements collected based by applying multiple techniques: testing, static analysis, modelling, etc.

Run-time assessment (and adaptation)

- Continuous monitoring
- Calculation of scores
- Planning of run-time changes
- Adaptation

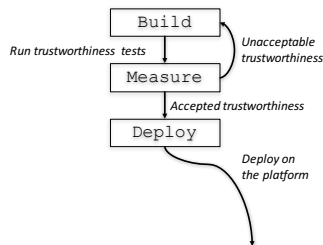
MAPE-K

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

12

PHASE 1: DESIGN-TIME ASSESSMENT



Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

13

PHASE 1 - STEP 1: ANALYSIS

Analyze the service under assessment

- Identify the relevant trustworthiness properties and their relative importance
 - e.g., in some cases privacy may be more relevant than performance, and in other cases the reverse may happen
- Can be based on predefined scenarios or using information about other services previously deployed
- Scenarios are used to take into consideration the circumstances of the service under assessment
 - Make the evaluation context-aware

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

14

PHASE 1 - STEP 2: MEASUREMENT

- Collect data for each relevant trustworthiness property
- Can be based on different techniques:
 - Running a set of tests
 - Performing static analysis
 - Manual or automated
- To ensure validity of the results, each individual assessment requires a deep understanding regarding:
 - Relevant attributes and properties
 - Thresholds
 - Various measurement instruments

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

15

PHASE 1 - STEP 3: CALCULATION

- Calculate the trustworthiness score by using the trustworthiness model
- This model is a representation of the process followed to perform the analysis of the obtained measurements
 - Based on a combination of weights of the attributes that determine the relative importance of each
- Assuring conformance to the service specification and meeting expectations
- Conflicting properties may be involved

Marco Vieira

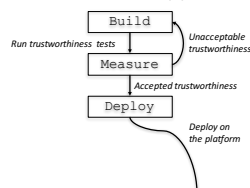
POSEIDON, July 10th, 2019, Coimbra, Portugal

16

PHASE 1 - STEP 4: DECISION

At this point a decision is to be made

- If the service under assessment achieves an acceptable level of trustworthiness, then it can be deployed
- Otherwise, further improvements should be applied and steps 1-4 repeated

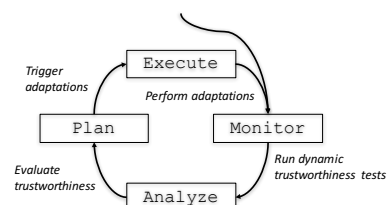


Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

17

PHASE 2: RUN-TIME ASSESSMENT



Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

18

PHASE 2 – STEP 1: MONITORING

Data related to the relevant trustworthiness properties defined are continuously collected

- Probes collect data that is managed and stored by a monitoring platform
- Tests may be executed to generate/collect data (active monitoring)
 - e.g. attack injection
 - Taking into account runtime aspects and constraints

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

19

PHASE 2 – STEP 2: CALCULATION

Calculate the trustworthiness score by using a trustworthiness model

– Similar to Step 3 of Phase 1

- Score serves two purposes:
 - Trustworthiness monitoring – e.g. information to users
 - Trustworthiness improvement
- If the level of trustworthiness of the service under assessment is not satisfactory:

Runtime mitigation actions should be planned and the system adapted

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

20

PHASE 2 – STEP 3: PLAN

- Select adequate adaptation solutions to improve trustworthiness
 - Estimation may apply
- Predefined adaptation strategies and tactics
- Multi Criteria Decision Making

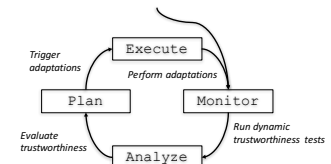
Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

21

PHASE 2 – STEP 4: CHANGE

- Adaptation engine
- Actuators to support the adaptation actions
- Phase 2 runs continuously while the service under assessment is being executed
 - Go back to Step 1...

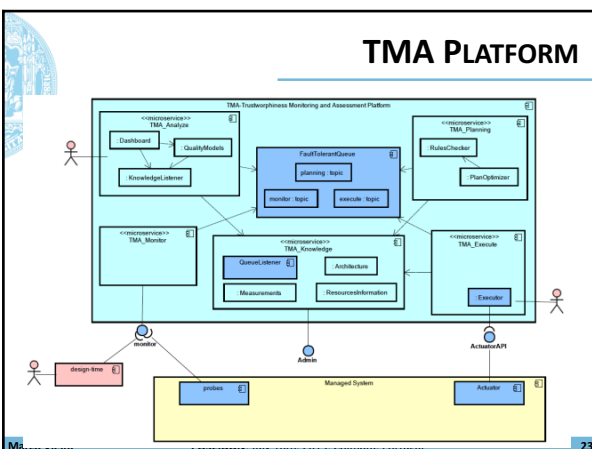


Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

22

TMA PLATFORM



Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

23

EXAMPLE: PERFORMANCE

Raw data:

- Timestamp for each request processed (begin & end)
- Collected over time

- Metrics:
 - Throughput
 - Response Time
- Trustworthiness Score
 - Performance Level
 - Different weights for Throughput and Response Time

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

24

EXAMPLE: PRIVACY...

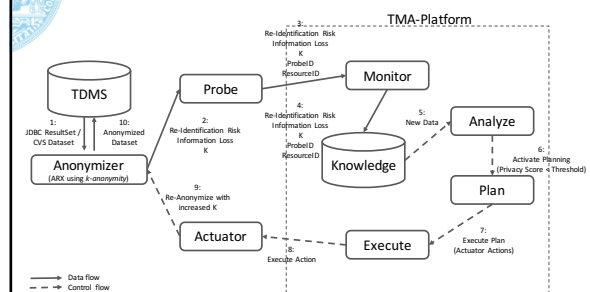
- Privacy from a trustworthiness perspective:
- Depends on how the data is stored
 - Data management services
- Depends on what is being done with the data
 - Data processing services

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

25

PRIVACY PROBE AND ACTUATOR



Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

26

CHALLENGES

- How to define attributes and sub-attributes for each trustworthiness property?
 - As well as the appropriate scores to characterize them
- How to define a set of scenarios that suggest a set of different weights for the different properties?
- How to define a measurement mechanism for each trustworthiness property?
 - Design-time and run-time
- How to build trustworthiness models based on the relevant attributes?

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

27

QUESTIONS?

Marco Vieira
Department of Informatics Engineering
University of Coimbra
mvieira@dei.uc.pt
<http://eden.dei.uc.pt/~mvieira>



UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Trust-IT Services Ltd
Communicating ICT to markets

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

UNIVERSIDADE DE COIMBRA

UNIVERSIDADE FEDERAL DE MINAS GERAIS

UNIVERSIDADE DE BRASÍLIA
Departamento de Ciência da Computação

TECHNISCHE UNIVERSITÄT DRESDEN

UNIVERSITY OF BIRMINGHAM
RESEARCH CENTER

UNICAMP
UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

quibim

DELL EMC

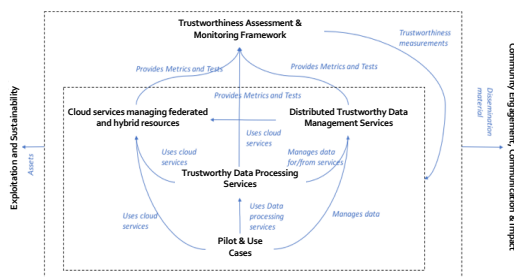
UNICAMP

Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

28

ACTIVITIES



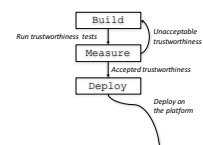
Marco Vieira

POSEIDON, July 10th, 2019, Coimbra, Portugal

29

HOW TO USE (DESIGN TIME)?


- Identify trustworthiness **properties** of interest
- Define trustworthiness **scores** to be computed for each property
- Define/adapt/reuse the **QMs** to compute the scores
- Identify the **data sources** for feeding the QMs
- Implement **probes** to collect data
- Deploy** probes and QMs
- Stimulate the system (run experiments)



Marco Vieira

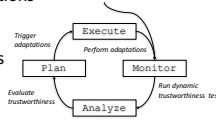
POSEIDON, July 10th, 2019, Coimbra, Portugal

30



HOW TO USE (RUN TIME)?

1. Identify trustworthiness properties of interest
2. Define trustworthiness scores to be computed for each property
3. Define/adapt/reuse the QMs to compute the scores
4. Identify the data sources for feeding the QMs
5. Implement probes to collect data
6. Identify potential **actuators/adaptations** to ensure trustworthiness
7. Implement **actuators** to perform adaptations
8. Define adaptation **rules**
9. **Deploy** probes, actuators, rules and QMs



```

graph TD
    Execute[Execute] --> Monitor[Monitor]
    Monitor --> Analyze[Analyze]
    Analyze --> Plan[Plan]
    Plan --> Execute
    Trigger[Trigger adaptations] --> Plan
    Perform[Perform adaptations] --> Execute
    Run[Run dynamic trustworthiness tests] --> Monitor
    Evaluate[Evaluate trustworthiness] --> Analyze
  
```

Marco Vieira
POSEIDON, July 10th, 2019, Coimbra, Portugal
31