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
certified 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

---

**CONSORTIUM**

---

**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
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.

---

**TRUSTWORTHINESS FRAMEWORK...**

Development
Build
Deployment
Measurement
Evolution
of trustworthy cloud resources, data management
and data processing services

---

**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

---
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

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

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 echocardiogram images

TRUSTWORTHINESS PROPERTIES

<table>
<thead>
<tr>
<th>Trust Prop.</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Ensuring integrity, availability, confidentiality, non-repudiation, and other security properties.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Ensuring that sensitive information is protected from unauthorized access and use.</td>
</tr>
<tr>
<td>Cohesion</td>
<td>Ensuring that the system operates consistently and reliably.</td>
</tr>
<tr>
<td>Isolation</td>
<td>Ensuring that the system is isolated from other systems to prevent unauthorized access and use.</td>
</tr>
<tr>
<td>Stability</td>
<td>Ensuring that the system remains operational and available despite failures.</td>
</tr>
<tr>
<td>Fairness</td>
<td>Ensuring that the system is fair and just, and that all users are treated equally.</td>
</tr>
<tr>
<td>Usability</td>
<td>Ensuring that the system is easy to use and understand.</td>
</tr>
<tr>
<td>Trustworthiness</td>
<td>Ensuring that the system is trustworthy, and that users can trust that it will behave as expected.</td>
</tr>
</tbody>
</table>

FROM PROPERTIES TO SCORES...

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

<table>
<thead>
<tr>
<th>Final Score</th>
<th>A1</th>
<th>A2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence</td>
<td>ws</td>
<td>ws</td>
</tr>
<tr>
<td>Evidence</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Evidence</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

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

TWO PHASES...

Design-time assessment
  - Assure specific properties before deployment
  - Development > Assessment > Development cycle until the expected level of trustworthiness is achieved
  - Measurements collected based on 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
PHASE 1: DESIGN-TIME ASSESSMENT

Build
Run trustworthiness tests
Measure
Accepted trustworthiness
Deploy
Unacceptable trustworthiness
Deploy on the platform

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

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

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

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

PHASE 2: RUN-TIME ASSESSMENT

Execute
Monitor
Analyze
Plan
Perform adaptations
Evaluate trustworthiness
Trigger adaptations
Run dynamic trustworthiness tests

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/collaborate data (active monitoring)
    - e.g. attack injection
    - Taking into account runtime aspects and constraints

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

PHASE 2 – STEP 3: PLAN
- Select adequate adaptation solutions to improve trustworthiness
  - Estimation may apply
- Predefined adaptation strategies and tactics
- Multi Criteria Decision Making

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...

TMA PLATFORM

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
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

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?

QUESTIONS?

- How to use (design 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. Deploy probes and QMs
  7. Stimulate the system (run experiments)
**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 actuations/adaptations to ensure trustworthiness
7. Implement actuators to perform adaptations
8. Define adaptation rules
9. Deploy probes, actuators, rules and QMs

---

**Trigger adaptions**

**Execute**

**Monitor**

**Analyze**

**Plan**

**Perform adaptions**

**Evaluate trustworthiness**

**Run dynamic trustworthiness tests**