Operational trustworthiness enabling technologies in software projects

Sandro Hartenstein, M. Sc.
Contents

• Introduction
• Usecase
• Method
• Results
• Outlook and Conclusion
Introduction
Introduction / Definitions

• **Trust**
  • personnel subjective belief of an acceptable outcome

• **Trustworthiness**
  • objective performance
    • observed system behaviour
    • monitored system development

• **Security**
  • protect entities against attacks and misuse
  • protect the access to resources
Introduction / OPTET

www.optet.eu

15 partners
6 Universities
3 SMEs

793,5 Person Months

Total Funding 7,1 M€
Total budget 10,7 M€

Start: 1st November 2012
Duration: 3 years
Ends: 31 October 2015

(http://cordis.europa.eu/project/rcn/105733_en.html)
Introduction / OPTET

OPTET Lifecycle (ATC, 2015, p. 13)
Introduction / OPTET

• key requirement is the determining of trustworthiness
  • What,
  • When and
  • How?

• How to manage, calculate, use and present the results?

• How to increase trustworthiness?
Introduction / OPTET / Attributes

- What?
Introduction / OPTET / Contexts

• When?

**Engineering**
- Source code
- Static code analyse

**Marketplace**
- Deployed software
- Configuration verification
- Testing

**Runtime**
- Running application
- Monitoring behavior
## Introduction / OPTET / Metrics

- How?

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Metric ID</th>
<th>Metric</th>
<th>Metric Computation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>APP-MAR-Storeencr-01</td>
<td>Percentage of encrypted user objects addressed</td>
<td>$x = \left(\frac{\text{sum of encrypted user objects}}{\text{sum of user objects}}\right) \times 100%$</td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td>APP-MAR-Digsig-01</td>
<td>% of activated functions that support the digital signature</td>
<td>$x = \left(\frac{\text{sum of activated functions that support the digital signature}}{\text{sum of activated functions}}\right) \times 100%$</td>
</tr>
</tbody>
</table>
**Introduction / OPTET / Tools**

**Design Phase**
- Secure System Designer
- System Analyser
- End-to-End Trustworthiness Calculator
- End-to-End Trustworthiness Evaluation Tool
- Trustworthy Development Enhancement Toolset
- Metrics tool

**Development Phase**
- Trustworthy Development Platform factory – Java
- Trustworthy Development Platform factory – OPA
- Trustworthy Development Enhancement Toolset
- Metrics tool

**Certification Phase**
- Certification Tool
- Trustworthy Development Enhancement Toolset
- Metrics tool

**Distribution and Deployment Phase**
- Trustworthy marketplace
- End-to-End Trustworthiness Evaluation Tool
- Trust and Trustworthiness Measurement
- Trust and Trustworthiness Management
- Mitigation
- Trustworthy Development Enhancement Toolset
- Metrics tool

**Maintenance Phase**
- Maintenance Portal
- User Behaviour Model
- Trust Metric Estimator
- Trust Evaluator
- Trustworthiness Evaluator
- Optimal Control Selector
- Trust and Trustworthiness Measurement
- Trust and Trustworthiness Management
- Mitigation
- Trustworthy Development Enhancement Toolset
- Metrics tool

How to manage, calculate, use and present the results?
Introduction / OPTET / TWbyD

• How increase trustworthiness in Software?
• Trustworthiness-by-design (TWbyD)
  • process extension
  • collection of
    • methodologies,
    • design patterns at architectural level,
  • and approaches to realizing the development of systems to be trustworthy (tools)
Operational trustworthiness enabling technologies in software projects
Sandro Hartenstein

Use-case
E- Health Application
Usecase / E-Health Application

• Idea
  • container for personal healthcare documents.
  • take pictures of documents
    • prescription
    • physician referral
    • medical findings

• Requirements
  • access via
    • mobile devices
    • webapplication
  • capture and show photos
  • secure data processing
  • easiest usability
Use case / E-Health
Usecase / E-Health

• special requirement
  • by law
    • special personal data (BDSG)
  • by customer
    • privacy
    • CIA for private health data
      • Confidential
      • Integer
      • Available

• need trustworthy software → use OPTET
Method

marked oriented exploitation
Method / Marked oriented exploitation

Commercial conversion

Full commercialisiation
Pending potential commercialisiation

Direct commercial transformation
Additional research activities
Additional non-research activities
Knowledge, technology integration an spill-overs
Technologie scanning

Indirect commercial transformation

Commercial transformation

(Ruhland & Romanow, 2013, p. 39)
Method / Trustworthiness related steps

1. Select Tools
2. Define process
3. Determine trustworthiness values
Results
# Results / Selected tools

<table>
<thead>
<tr>
<th>Design</th>
<th>Development</th>
<th>Distribution</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure System Designer</td>
<td>OPA factory</td>
<td>Trustworthy Development Enhancement Toolset</td>
<td>Maintenance Portal (CEP in FI-Ware)</td>
</tr>
<tr>
<td>End-to-End TW Calculator</td>
<td>Trustworthy Development Enhancement Toolset</td>
<td>Metrics tool</td>
<td>TW Measurement (CEP in FI-Ware)</td>
</tr>
<tr>
<td>End-to-End TW Evaluation tool</td>
<td>Metrics tool</td>
<td></td>
<td>Metrics tool</td>
</tr>
</tbody>
</table>
Results / Development process

Management of Trustworthiness

determine trustworthiness
set trustworthiness requirements

Design
- architect the software with UML
- model the System in SSD
- measure parameters for End-to-End Evaluation Tool

Development
- generate source code in factory
- extend source code and resource
- measure tw parameters for metrictool

Distribution
- Deploy to AppStore
- Deploy to Applicationserver
- measure tw parameters for metrictool

Maintenance
- set maintenance portal
- configure tw measurement

10/17/2016 EICAR 2016 "OPTET in software projects" Sandro Hartenstein
Results / Use case

Trustworthiness Attributes

- Accountability
- Auditability/Traceability
- Confidentiality
- Integrity
- Safety
- Non-Repudiation
- Compliance with standards
- Compliance with regulations
- Compliance with User expectations
- Data Integrity
- Data Reliability
- Data Timeless
- Data Validity
- Data Completeness
- Data Consistency
- Openness
- Reusability
- Change Cycle/Stability
- Completeness
- Functional Correctness
- Composability
- Software Complexity
- Security
- Usability
- Usability
- Dependability
- Reusability
- Flexibility/Robustness
- Reliability
- Scalability
- Maintainability
- Provability
- Flexible continuity
- Response Time
- Throughput
- Level of Service
- Satisfaction
- Learnability
- Effectiveness
- Efficiency of Use
- Predictability
- Accessibility
- Content Accessibility
- Accuracy
- Availability
- Privacy
- Cost
- Cost
- Privacy

High priority
Mid priority
Outlook and Conclusion
Outlook

- design phase
- first draft of SSD model
Conclusion

• Cons
  • additional work to do
    • set up tools
    • Introduce methods
  • additional management
    • measure, calculate, process and interpret trustworthiness values

• Pro
  • faster & better implementation
    • tools
    • methods
    • management of trustworthiness
  • market acceptance
    • transparency software development process
    • transparency requirements that address trustworthiness
  • trustworthy software
Thank you for your attention

Questions?

Literature


