Modeling, Specifying, Discovering, and Integrating *Trust* into Distributed Real-time and Embedded (DRE) Systems (Status Report)

Lahiru S. Gallege, Dimuthu U. Gamage, James H. Hill, Rajeev R. Raje
{lspileth, dcundupi, hillj, raje}@cs.iupui.edu

William McKeever and Steven Drager
(AFRL)
Long-term Objectives

- How to model and incorporate trust during early phases of a DRE system’s software lifecycle?

- How to represent, select and compose trusted services to build a specific DRE systems from a collection of repositories?

- How to create models that can predict the trust-related properties of a DRE system using the trust-related attributes of individual services?

- How to automate, where applicable, the composition of the selected individual services, thereby preserving the trust attributes in the ensemble created out of these services?

- How to provide a comprehensive approach, based on continuous integration testing, for validating a DRE system composed out of trusted individual services?

- How to empirically validate the outcomes of the proposed research by creating various prototypical systems?
Status (S²ERC Showcase 2011 November)

- Performed a comprehensive survey of approaches that have been proposed to model trust in distributed systems

- Defined the trust of a service using Subjective Logic
  - Trust of a service as a tuple of \((\text{Belief}, \text{Disbelief}, \text{Uncertainty})\)
  - Trust of a service is measured from both internal and external views (i.e., both developers’ and reviewers’ views)

- Devised preliminary trust composition rules, based upon common interaction patterns of services, to predict the overall trust of a composed system
  - Case study from Distributed Tracking System
Trust of an Individual Service

- How to identify internal views (developer’s view) of trust?
  - A list of artifacts which a developer could use as evidences

- How to identify external views (Reviewers’ view) of trust?
  - Use of ratings, reputation, and comments as evidences

### Compatibility of Evidences (E) included in views from Developers (D) and Reviewers (R)

#### Scenario 1: In Agreement

<table>
<thead>
<tr>
<th>Version, Time</th>
<th>Internal Views</th>
<th>External Views</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_1, t_1$</td>
<td>$E_D(B,D,U)_D$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t_2$</td>
<td></td>
<td>$E_R(B,D,U)_R$</td>
<td></td>
</tr>
<tr>
<td>$t_3$</td>
<td>$E_D(B,D,U)_D$</td>
<td>$E_R(B,D,U)_R$</td>
<td>Agree</td>
</tr>
</tbody>
</table>

**Case 1: Converge**

- $E_D(B,D,U)_D$ → $E_R(B,D,U)_R$

#### Scenario 2: In Disagreement

<table>
<thead>
<tr>
<th>Version, Time</th>
<th>Internal Views</th>
<th>External Views</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_1, t_1$</td>
<td>$E_D(B,D,U)_D$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t_2$</td>
<td></td>
<td>$E_R(B,D,U)_R$</td>
<td></td>
</tr>
<tr>
<td>$t_3$</td>
<td>$E_D(B,D,U)_D$</td>
<td>$E_R(B,D,U)_R$</td>
<td>Disagree</td>
</tr>
</tbody>
</table>

**Case 2: Diverge**

- $E_D(B,D,U)_D$ ↔ $E_R(B,D,U)_R$
Trust of a Composed DRE System

Case Study from Android Market: A Personalized Travel Planner

- Each type of services has many instances (e.g., Traffic)

Internal View
- Design By Contract
- Best Practices
- Features:
  - Real-time traffic maps
  - Detailed incidents reports
  - Traffic camera images
  - Location aware

External View
- Average User Ratings
- User Comments

Overall Trust \((T_s) = f(T_{iv(s)}, T_{xv(s)})\)
Composing Security-related Properties

Gatekeeper Pattern

Composed Trust: \( T(S1) \)

Examples of Security-related Properties
- Authentication
- Authorization
- Confidentiality
  - Separability
  - Non-Interference
  - Non-Inference
- Integrity

Sequence Pattern

Trust Operator: Conjunction

Split/Join Pattern

Discriminator Pattern

Trust Operator: Disjunction

Examples of Security-related Properties
- Authentication
- Authorization
- Confidentiality
  - Separability
  - Non-Interference
  - Non-Inference
- Integrity
**Trusted Service Composition**

- Trust Operator associated with a property depends on the composition operator which in-turn depends on the nature of the property and the composition pattern.

<table>
<thead>
<tr>
<th>Composition Operator</th>
<th>Trust Operator</th>
<th>Composition Example</th>
<th>Trust Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existential (∃)</td>
<td>Disjunction (∨)</td>
<td>∃ (P_{s1}, P_{s2},..., P_{sn})</td>
<td>P_{s1} ∨ P_{s2} ∨ ... ∨ P_{sn}</td>
</tr>
<tr>
<td>Universal (∀)</td>
<td>Conjunction (∧)</td>
<td>∀ (P_{s1}, P_{s2},..., P_{sn})</td>
<td>P_{s1} ∧ P_{s2} ∧ ... ∧ P_{sn}</td>
</tr>
<tr>
<td>Minimum</td>
<td>Conjunction (∧)</td>
<td>∀ (P_{s1}, P_{s2},..., P_{sn})</td>
<td>P_{s1} ∧ P_{s2} ∧ ... ∧ P_{sn}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B( x &gt; r) = 1 - Φ_{μ,σ} (P_{s1},..., P_{sn})</td>
<td>min (P_{s1}, P_{s2},..., P_{sn})</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T (P_{1} &gt; r) = T (P_{s1} &gt; r) ∧ ... ∧ T (P_{sn} &gt; r) where B(P_{1} &gt; r) = 1 - Φ_{μ,σ} (P_{s1},..., P_{sn})</td>
<td></td>
</tr>
<tr>
<td>Maximum</td>
<td>Disjunction (∨)</td>
<td>∃ (P_{s1}, P_{s2},..., P_{sn})</td>
<td>P_{s1} ∨ P_{s2} ∨ ... ∨ P_{sn}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B( x &lt; r) = Φ_{μ,σ} (P_{s1}, P_{s2},..., P_{sn})</td>
<td>max(P_{s1}, P_{s2},..., P_{sn})</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T (P_{1} &lt; r) = T (P_{s1} &lt; r) ∧ ... ∧ T (P_{sn} &lt; r) where B(P_{1} &lt; r) = 1 - Φ_{μ,σ} (P_{s1},..., P_{sn})</td>
<td></td>
</tr>
<tr>
<td>Addition (+)</td>
<td>Disjunction (∨)</td>
<td>∃ (P_{s1}, P_{s2},..., P_{sn})</td>
<td>P_{s1} ∨ P_{s2} ∨ ... ∨ P_{sn}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B = ∑ N_{μ,σ}</td>
<td>P_{s1} + P_{s2} + ... + P_{sn}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B(p) = ∑ N_{μ,σ}</td>
<td></td>
</tr>
<tr>
<td>Multiplication (*)</td>
<td>Conjunction (∧)</td>
<td>∀ (P_{s1}, P_{s2},..., P_{sn})</td>
<td>P_{s1} ∧ P_{s2} ∧ ... ∧ P_{sn}</td>
</tr>
</tbody>
</table>
Conclusions

- Internal view of trust of an individual service is quantified using the $<b, d, u>$ model
  - Standard list of internal artifacts and associated practices

- External view of trust of an individual service is also quantified using the $<b, d, u>$ model
  - Reputation, past history, and outside reviews

- The overall trust of a service combines both the views
  - Theory of evidence

- Trust of an ensemble of services is predicted using individual $<b, d, u>$ values and associated composition patterns
  - Composition operators
  - Theory of evidence
Future Work

• How to enhance the belief, disbelief and uncertainty-based trust model for software services and their ensemble?

• How to formalize and incorporate trust during a DRE system’s software lifecycle?

• How to discover trusted services from a collection of repositories that can form the fundamental building blocks of specific DRE systems using this enhanced model?
Thank You!
Any Questions/Comments?

IUPUI
DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE
SCHOOL OF SCIENCE
A Purdue University School
Indianapolis

Undergraduate Research Laboratory

User Reviews

Average rating:
4.1

42,525

INSTALL

Shake To Charge Battery
Life Mobile

Jennifer on April 17, 2012 (Motorola Droid RAZR with version 1.2)★★★★ Never again
This is dumb. Does NOT work for me. I tried... I have a Droid razr 2 so my battery dies quick. Would be nice if really worked... tried twice it drained my battery 10% in one min

Tomaz on April 12, 2012 (HTC Desire with version 1.2)★★★★★ Superb!
Yes! Try to sink it in a glass of water and then shake it! It works faster! No need for charger any more!