Aniketos: Ensuring Trustworthiness and Security in Service Composition

Exploitation and Impact

David Llewellyn-Jones
Zeta Dooly
Marina Egea González

http://aniketos.eu

6th September 2012
Effectsplus Clustering Event, Padua, Italy
Contents

- Aniketos overview
  - Security policies
  - Trustworthiness
  - Threats
  - Composition and adaptation
  - Social-Technical Modelling

- Exploitation and Impact
  - Tutorials and training
  - Demonstrations
  - Community building and standardisation
  - Dissemination and exploitation

- Case studies
Aniketos Project

- **Main objective**
  - Help establish and maintain trustworthiness and secure behaviour in a dynamically changing environment of composite services

- **ICT FP7 Objective 1.4**
  - Secure, dependable and trusted infrastructures

- **Duration**
  - August 2010 until February 2014

- **Website**
  - [http://aniketos.eu](http://aniketos.eu)
Aniketos Workflow

Service developers

Compose
- Specification, discovery, composition and validation support based on trustworthiness/security properties, metrics and contracts
- Relevant threat awareness

Service providers

Provide
- Trust and security monitoring
- Threat notification

Service end users

Invoke
- End user trust assurance and acceptance
- Identification of responsible party

Adapt/recompose
- Self-protection
- Trust evaluation
- Security validation

Component change
Change of threats
Change of environment

Design-time

Runtime

Effectsplus, Padua, Italy, 6 September 2012
Security Policies

- Define properties of a service or service composition
- Used in several forms
  - Service developer/provider’s claimed properties for a service
  - Service user’s desired properties
  - Contract agreed by both
- Technologies
  - Written using ConSpec

```xml
<specification>
  <scope>session</scope>
  <rule>
    <before>
      <identifier>*</identifier>
    </before>
    <perform>
      <reaction>
        <guard>
          <invocation>
            <identifier>
              eu.aniketos.predicates.dSOD
            </identifier>
            <argument>
              <identifier>
                s1.method1
              </identifier>
            </argument>
            <argument>
              <identifier>
                s2.method2
              </identifier>
            </argument>
          </invocation>
        </guard>
        <update/>
      </reaction>
    </perform>
  </rule>
</specification>
```
Trustworthiness

- Security × Contract × Trust paradigm
  - Service properties monitored against policy
  - Violations affect trust
  - Trustworthy services avoid verification step
- Technologies
  - Trust monitoring
  - Trust composition
  - Security verification

Secured Composition Plans

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Trustworthiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>compositionPlan1</td>
<td>C...</td>
<td>10.6</td>
</tr>
<tr>
<td>compositionPlan2</td>
<td>C...</td>
<td>20.5</td>
</tr>
<tr>
<td>compositionPlan3</td>
<td>C...</td>
<td>30.6</td>
</tr>
</tbody>
</table>

Effectsplus, Padua, Italy, 6 September 2012
Threats

- Runtime and environmental threats
  - Changing threats may cause user alert or policy change
- Threat repository
  - Community list of relevant threats
  - Threats associated with possible solutions
- Runtime threat monitoring
  - Based on information in threat repository and policy
Deployment and Adaptation

- Service Composition Framework
- Compositions specified using BPMN
- Services replaced to maintain policy
Socio-Technical Modelling

- Architectural approach for specifying
  - Service composition
  - Security policy
  - Trustworthy requirements
  - Threat requirements
- Goal-oriented modelling
Workflow

- Incorporates comprehensive workflow
- Relies on significant input
  - From developers, providers and end-users
  - Commercial or community
- Ecosystem
  - BPMN service compositions
  - ConSpec policy files
  - Trust management
  - The actual services
- Services may be ‘Aniketos compliant’
Exploitation and Impact

- Four fronts
  - Tutorials and training
  - Demonstrations
  - Community building and standardisation
  - Dissemination and exploitation

WP8: Tutorials and training
WP9: Demonstration
WP10: Community building and standardization
WP11: Dissemination and Exploitation
WP12: Project management

Effectsplus, Padua, Italy, 6 September 2012
Tutorials and Training

- Led by SearchLab
- Building up standardised documentation
  - Standard templates for all prototype deliverables
  - Automated document generation tools
- Workshops and events
  - February 2011 – STS and S×C×T
  - July 2011 – STS Modelling Language
  - More planned

3 Code commenting

As a general guideline, Doxygen and Javadoc interpret all comments that start with `/**`. Therefore the usual comment block targeting reference manual documentation should look like:

```
/**
 * Write your comment here meant to be
 * included in the automatically generated
 * reference manual. All annotations should
 * be also inserted into these blocks.
 */
```

Special annotation commands for Javadoc that can be used are enlisted on the following pages:

- [http://www.stack.nl/~dimitri/doxygen/commands.html](http://www.stack.nl/~dimitri/doxygen/commands.html)

For Javadoc see the following page for further information about some special commands:


In general we would encourage using only those commands that are compatible with both documentation tools, however – as Doxygen will be used for the generation of external deliverables – it is acceptable to use annotation that is not supported by Javadoc.

Annotations refer forward to the code element that follows the comment block. The exception to this rule is the Doxygen-only annotation that refers backwards to the previous element by using `<`, as described in:

- [http://www.stack.nl/~dimitri/doxygen/docblocks.html](http://www.stack.nl/~dimitri/doxygen/docblocks.html)

Besides directly commenting and annotating certain elements of the code (classes and methods, see section 3.1.1), we would encourage developers to annotate their authorship of the code by using the `@author <name>` annotation in the following form:

```
/**
 * Comments regarding the code element.
 * @author John Smith
 */
```

3.1.1 How to comment various code elements

In this section we will list the code elements that are mandatory to be commented for Doxygen/Javadoc, along with possible ways to annotate the elements.
Demonstrations

- Led by Italtel
- Trade shows and conferences
- Demo events
  - February 2012 – Internal Aniketos
  - May 2012 – Selex Elsag demo
  - July 2012 – Wind demonstration
  - July 2012 – SummerSOC
  - More planned
- Building software VMs

Effectsplus, Padua, Italy, 6 September 2012
Community Building

- Led by TSSG
- Aim to build communities
  - Contribute to standardisation
  - Generate interest
  - Foster open source community
- Targeting open source alone is risky
  - Requirement for external input
  - Capitalise on social networking
  - Github, YouTube, LinkedIn, Twitter, etc.
- Aim to combine both commercial and open source
Dissemination and Exploitation

- Led by ATOS
- Publications
- Case Studies
  - Future telecom services
  - eGovernance: land buying
  - Air traffic service pool
- Demos
- Real-world deployment with project partners
Future Telecoms Scenario

Bob accesses the WebShop application in order to purchase an electronic item he wishes.

The end user (Bob) owns a mobile device which is equipped with a GPS receiver and a presence enabled VoIP client when accessing the web portal of his TLC Operator.

The services involved are:
- a. WebShop for general electronic commerce access;
- b. StoreLocator for making users choose the store where to pick up items selected;

Bob requests the help of an assistant by starting a click-to-call VoIP communication.

Bob selects option 2) for automatic store localization. By doing so a service recomposition is started...

...to collect Bob’s current position information and to generate maps and addresses of the stores which are closer to Bob.

Bob is finally asked to confirm his mail address (that was retrieved through the IdP) to inform him when he can pick-up the purchased item.

He decides to purchase the item he was interested in.

The StoreLocator service gives users two options, 1) a manual selection of the pick-up stores that can be selected from an offered list; 2) letting StoreLocator service propose a list of closest stores.

Effectsplus, Padua, Italy, 6 September 2012

ANIKETOS
Audience Reached

- Commercial Sector (ICT Industry)
  - Software developers and providers
  - Service architecture providers
  - Security Experts
  - ICT providers, IT vendors
  - Internet Service Providers, Cloud Providers
  - End-users from Safety and Security Critical Domains

- Aniketos strategic partners
  - Other EU projects working in similar domain
  - EU technology platforms
  - Other research initiatives and big IT companies

- Academia
  - Scientists, Students (especially, Master and PhD students)

- European Commission, European Society

Effectsplus, Padua, Italy, 6 September 2012
Industrial Audience

- **DEEPBLUE**
  - Air Traffic Management experts, industries, practitioners and researchers (thanks to Aniketos ATC case study)

- **SELEX ELSAG**
  - Own customers
  - FinMeccanica companies
  - R&D managers and employees

- **SAP**
  - Academia
  - SAP internal stakeholders
  - external partners and SAP developers

- **WIND**
  - Employees, technical and marketing departments

Effectsplus, Padua, Italy, 6 September 2012
Industrial Audience

- **Atos**
  - Internal research and innovation department
  - Atos internal stakeholders
  - Business development director
  - FI-WARE, ChoREOS, NESSoS, *etc.*
  - Inter industry-academia event co-organizer (MDSec @ MoDELS 2012)
  - Joined new group addressing standardization of trustworthy, secure composable services

- **EM**
  - Greek public sector and government
  - Athens (previous) city council and other IT companies

Effectsplus, Padua, Italy, 6 September 2012
Industrial Audience

- **SEARCH-LAB**
  - Software developers
  - Presented in several inter industry-academia scientific events

- **THALES**
  - Technical teams
  - Centre for evaluation of the security of information technology, software engineers
  - Security experts, head of the security architecture unit, security consultants, technical and strategy managers

- **ITALTEL**
  - Technical and marketing departments
  - Intranet community
  - Internet users

Effectsplus, Padua, Italy, 6 September 2012
Academic Audience

- Targeting academics
  - Workshops, seminars, conferences
    - Submitters or organisers for more than 40 events
  - Organizers or PC members
    - Around 20 events
  - Papers
    - Over 40 papers on Aniketos research results (out of 80 submissions)

- Targeting industry
  - Participation in around 20 events
  - Including worldwide event reaching global SAP developer community

Effectsplus, Padua, Italy, 6 September 2012
## Academic Partners

<table>
<thead>
<tr>
<th>Event Type</th>
<th>CNR</th>
<th>LJMU</th>
<th>PLUS</th>
<th>SINTEF</th>
<th>Tecnalia</th>
<th>TSSG</th>
<th>UNITN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events participated/organized</td>
<td>5</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>3</td>
<td>7</td>
<td>15</td>
</tr>
<tr>
<td>Participated Master, PhD programs, Seminars, consultancy</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>Press Release</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Platforms/clusters/standardization</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Papers</td>
<td>11</td>
<td>5</td>
<td>1</td>
<td>9</td>
<td>12</td>
<td>12</td>
<td>9</td>
</tr>
</tbody>
</table>

Effectsplus, Padua, Italy, 6 September 2012
Promoting Website Visits

- Website intended to be main channel
  - Currently role less crucial
  - Mainly due to lack of technical and training material
  - Strategy therefore to publish more material
- Publish multimedia content when ready
  - Embedded videos being shown on web front page
    - Embedded from Aniketos YouTube channel
  - Deliverables
  - Demo material on success stories
  - Broadcast new achievements via social channels
- Aim to cross-link between project websites
Outreach Boost Plan

Key ideas to boost outreach

Key message specification and communication

ANIKETOS

Effectsplus, Padua, Italy, 6 September 2012
Outreach Boost Plan

Key results

Key outputs

Effectsplus, Padua, Italy, 6 September 2012
Outreach Boost Plan

- Project Internal collaboration
  - Training
    - External Collaboration
      - Getting involved in coordination actions
        - Service orientation
          - Security
            - Target TOP venues
              - Academic outlets

- Promote results in web service developer security training
- Joint event with other R&D projects on same topics
- Share it

- Exploit existing social media / forums
  - Social group for discussions + inviting externals
  - List of 20 Security experts to include in discussions

- Effective usage of social networks
  - Syndicate Material (automatically)
  - More distributed Noise

- Appealing (not technical) videos to be shared
  - Upload videos and put to the web
    - YouTube
  - Inspiring/cool YouTube content
    - Blog Entries
      - Website

- Material Assets
  - Develop USB Keys (logo, loaded with Aniketos dissemination)
    - For industrial whitepapers
      - Add articles to online document repositories
        - TechTarget
      - Write joint white paper on service security

Outreach Boost

Key Message
- Key Results
- Key Output

ANIKETOS

Effectsplus, Padua, Italy, 6 September 2012
Conclusion

- Four targeted areas for increasing impact
  - Tutorials and training
  - Demonstrations
  - Community building
  - Dissemination and exploitation
- Dissemination through outreach boost
  - Key message
    - Targeted user groups
  - Key results
    - Success story publication
  - Key outputs
    - Code and business models
  - Improved sharing
Effectsplus, Padua, Italy, 6 September 2012