Towards an Engineering Process for Certified Multilayer Cloud Services

Work-in-progress

ACSAC 2013 - Layered Assurance Workshop
New Orleans, Louisiana, USA. 10th December 2013

Authors:
Rajesh Harjani, Marcos Arjona,
Antonio Muñoz, Antonio Maña (speaker)

University of Malaga, Spain
{rajesh, marcos, amunoz, amg}@lcc.uma.es
CUMULUS: Certification infrastrUcture for MUlti-Layer cloUd Services

- EU-Funded Research Project
- 8 Partners from across Europe

http://www.cumulus-project.eu/
Motivation

- Cloud computing is interesting from the economic, operational and even energy consumption perspectives...
- but it still raises concerns regarding the security, privacy, governance and compliance of the data and software services offered through it.
- It is difficult to verify security properties of the different types of applications and services available through cloud technology because of two facts:
  - (i) that the provision and security of a cloud service is sensitive to potential interference between the features and behavior of all the inter-dependent services in all layers of the cloud stack, as well as dynamic changes in them; and
  - (ii) that current cloud models do not include support for trust-focused communication between layers.
The concept of security certification provides an appropriate and robust mechanism for supporting assurance and compliance...

but there are two important problems:

P1 certification has traditionally been represented for humans and has not been able to support automated processing of certifications (i.e. verification, selection based on certifications, etc.); and

P2 certification cannot not provide dynamic proofs of the status of a system at runtime, which are extremely important in a dynamic, heterogeneous and unpredictable scenario such as cloud computing.

While recent advances (by ASSERT4SOA project) have solved P1 by producing computer oriented formats, processes and tools to support the automated validation of certifications and the selection of services based on their certificates (a computer-oriented form of certification called ASSERTS); P2 does not currently have a satisfactory solution.
Layered system and approach

- Applications
- Services
- Cloud Supporting Infrastructure
- Native OS
- Hardware

Certification

Security Certificate depends on

Security Certificate

Security Certificate depends on

TC Proof
Our focus

- Engineering and developing CUMULUS-aware systems (services and applications) requires specific and novel considerations to be taken into account
  - Systems will be composed not only based on functional aspects, but also on **security aspects (properties, threats, risks,...)**
  - Trust is established by means of certificates
  - Components of a system may change without the knowledge or control of other components
Main scientific challenges and approaches

- Facilitate the engineering of cloud-supported systems
  - Specification of security requirements
  - Propagation of requirements to services used in the design
  - Security-driven selection of services
  - Dynamic reconfiguration of system
  - Certification of services

- This implies
  - Derive certification requirements from security requirements
    - Use PROPERTIES as the pivotal element, complemented with expert knowledge about the relations between those properties and other aspects in a specific domain
  - Facilitate the certification-oriented evaluation of continuously evolving systems
    - Follow the approach we could call "engineering for certification"
      - Engineering activities produce results that facilitate certification by external authorities
      - Based on robust traceability mechanisms
  - Define an engineering metamodel that is expressive and flexible enough in order to address heterogeneous security engineering requirements
    - Use the concept of DOMINAN to allow different interpretations and context-specific issues to be represented
Main technical challenges

- Develop CUMULUS service engineering tools supporting the engineering process
  - In a way that facilitate the daily work of designers and developers of cloud systems → Integrate the tools in existing development environments

- Develop security engineering **metamodels** to support the operation of the tools

- Develop a distributed **repository** to store metamodels

- Support the development of CUMULUS-enabled applications
  - Develop code (libraries) to perform the common tasks of interacting to the framework and using CUMULUS Certificates
CUMULUS engineering vision

CUMULUS Consortium

CUMULUS Certification Metamodel

CUMULUS Framework Specification

Certification Authority

Cloud Provider

Cloud System Developer

CUMULUS-enabled cloud

CUMULUS Framework Instance

CUMULUS-enabled cloud

Certification requirements

CUMULUS application

End user

User preferences

CUMULUS Certificate

Covers both application and service developers
Layered Modeling Framework: Metamodels

UML Metamodel

Core Security Metamodel (CSM)

Domain Security Metamodel (DSM)

System Model

Final Review - Málaga, June 20th -21th 2013
CUMULUS Engineering Process

Cumulus Consortium
- Cumulus Certification Metamodel
- Cumulus Engineering Process
- DSM Concept
- CSM Concept
- Standard CSM

Security Expert
- Security & Certification Knowledge

Application Developer
- Application Knowledge

Service Developer
- Implementation Knowledge

Certification Authorities
- Certification Knowledge
- CA repository
- Certification model
- SAPs

Cumulus Eng. Repository

Engineering level

DSMs

Cumulus Application

Certification Services
Key developments

● **Security requirements specification in system models**

● **Among the main scientific challenges mentioned, we highlight the transformation of security requirements into Certification Requirements.**
  
  ▶ To perform this transformation we have defined the concept of *Service Assurance Profiles* (SAPs).
  
  ◆ These artifacts, contained in the DSMs, will link the assets subject of protection with the security properties provided by the DSM.
  
  ◆ A SAP is like a partially complete certificate including semantic rules about its content.
    
    - They are provided by Certification Authorities.

  ▶ The transformation of security requirements into Certification Requirements is semiautomatic.
  
  ◆ Cloud System Developers will choose suitable SAPs, from the DSMs, for fulfilling a certain security property.

● **First version of the engineering tool planned for Q1 2014.**
  
  ▶ Will be made publicly available
Thanks for your attention!
Questions?