Towards Novel Certification Models in Cloud Infrastructures
(the CUMULUS approach)

Professor G. Spanoudakis
School of Informatics
CSP Forum,
18-19 April 2013, Brussels
Outline

- Cloud Security – Still a problem?
  - Provider perspective & counter arguments
  - Evidence: incidents and perceptions
  - Security audit & risk assessment

- CUMULUS
  - Overall vision
  - Hybrid, multi-layer and incremental certification
  - New certification models
  - Infrastructure
  - Interoperability and standards

- Conclusions
Cloud security

Still a problem?
Cloud security – the arguments

Still a problem?

The provider’s argument:

Increased security due to

• Concentration and availability of expertise

• Use of cutting edge security solutions

• Increased controls

• Regular audits
Cloud security – the arguments

Still a problem?

The provider’s argument:

Increased security due to

• Concentration and availability of expertise
• Use of cutting edge security solutions
• Increased controls
• Regular audits

Counter arguments:

• Breach of data integrity, confidentiality\textsuperscript{[1,2,3]} and privacy\textsuperscript{[4]}
• Spamming, cross-site scripting attacks\textsuperscript{[5]}
• Denial-or-service (DoS) attacks\textsuperscript{[6,7]}
• Reduced application and data availability\textsuperscript{[2]}
• Authentication, authorization and accounting (AAA) vulnerabilities\textsuperscript{[2,1]}
• VM vulnerabilities (e.g., heap overflow, abnormal termination of VM processes) following stress testing and inspection\textsuperscript{[27]}
Cloud security – the evidence

Some incidents

- **Amazon**
  - 24/12/2012: outage of Elastic Load Balancing Service (load balancing of virtual servers) for 10Hrs (affected Netflix)
  - 04/2011: EC2 cloud suffered multiday outages causing loss of availability and data (affected Reddit/36Hrs, Foursquares, Hootsuite and Quora/48Hrs)

- **Microsoft Azure**
  - 28/2/2012: unavailability (24Hrs) due to leap year affecting, plus up to 24 more Hrs to restore (affected UK G-Cloud CloudStore)

- **Megaupload**
  - 01/2012: cloud storage service suspension due to copyright infringement (effect: 180m users / 25 petabyte); co-tenants permanent data loss & reputation damage

- **Other**
  - 06/2009: 0-day vulnerability in HyperVM (LxLabs) server virtualisation; exploited to delete 100,000 websites using it for hosting purposes
Industry Perceptions:

- security and privacy concerns:
  - block uptake of cloud computing completely for 10% of European enterprises, and
  - limit it for another 30% of enterprises\(^{[25]}\)
Security Audits & Risk Assessment

- Frameworks for auditing company IT controls:
  - SSAE 16 [31]
  - ISAE 3402 [32]
  - COBIT[34]

- Frameworks for assurance of security management practices:
  - NIST 800-53 Rev 4[36]
  - ISO 2700x : assessing the information security risk of IT systems
  - (on-going) extension to 27017 to provide cloud specific controls

- Some with an explicit focus on cloud, e.g.:
  - ENISA’s Cloud Computing Information Assurance Framework[35]
  - Security recommendations for cloud providers by German Federal Office for Information Security (BSI)
  - COSO[33]
Security Audits & Risk Assessment

- Frameworks for auditing company IT controls:
  - SSAE 16 \[^{31}\]
  - ISAE 3402 \[^{32}\]
  - COBIT\[^{34}\]

- Frameworks for assurance of security management practices:
  - NIST 800-53 Rev 4\[^{36}\]
  - ISO 2700x: assessing the information security management of IT systems
  - (on-going) extension to 27001 to provide cloud specific controls

- Some with an explicit focus on cloud, e.g.:
  - ENISA’s Cloud Computing Information Assurance Framework\[^{35}\]
  - Security recommendations for cloud providers by German Federal Office for Information Security (BSI)
  - COSO\[^{33}\]

**BUT**

Low degree of automation
Monitoring is not continuous
Cloud Certification – An answer to the problem?

- Software certification is not new (e.g., Common Criteria model) BUT
  
  i. Covers monolithic systems
  
  ii. Targets humans → certificates
      a. not amenable to automated processing
      b. cannot be used for automated (and possibly on-fly) system component selection/replacement, verification etc.)
  
  iii. Cannot cope with changes to system structures and the operational environment

- Recent work on SOA certification (Assert4SOA project[22]) covers (i)-(iii) in some circumstances but not in all and not for cloud services, e.g.:
  
  - Schema for specifying machine processable service certificates
  - Ontologies for annotating certificates
  - Certificates aware software service discovery and SaaS level composition[23]
The CUMULUS approach
CUMULUS - overview

- EU funded STREP (medium size targeted) research project (Proj. no. 318580)
- Total budget: €4.3m EU contribution: ~ €3m funding
CUMULUS – Overall vision

Development of an integrated framework of models, processes, and tools supporting the certification of security properties of infrastructure (IaaS), platform (PaaS) and software application layer services (SaaS) in clouds.

Use of multiple types of evidence for security assessment including:
- testing data
- monitoring data
- trusted computing proofs

Use of different models for security assessment:
- hybrid,
- Incremental, and
- multi-layer security certification.
Hybrid certification

What?

Certification based on combination of different types of evidence:
- testing data
- monitoring data
- trusted computing proofs for the hardware elements of cloud infrastructures

Why?

Some properties might be certifiable using a combination of evidence types
Hybrid certification – examples

- The availability of a SaaS layer service S may be certified by a certificate based on:
  - test data for the service and
  - a TC proof for the configuration of the hosting cloud infrastructure (to ensure that the infrastructure where the service is deployed is the same as that for which test data were obtained)

- Hybrid certificate for a SaaS service integrity based on test data and continuous monitoring in real operating conditions
Multi-layer certification

What?

- Certification based on a combination of certificates of inter-dependent services (as opposed to simply “evidence”) at different layers of the cloud stack
- Note: dependencies can be bottom-up, top-down or side-level

Why?

- Security properties are affected by such dependencies
- Liability or reasoning restrictions (e.g., inability to obtain the direct evidence required for property assessment) require making assessments based on certificates rather than direct evidence
Multi-layer certification – examples

- The integrity of data-at-rest of a software service $S_1$ using a cloud storage service $S_2$ could be certified on the basis of a certificate regarding the correct implementation of a “proof-of-storage” protocol by $S_2$.

- The availability of a messaging service in a cloud federation may be certified on the basis of certificates regarding DoS-resilience of the hosting node(s) in the federation.

- A data-in-process integrity certificate of a SaaS layer service requires TCP based certificate for hypervisor to ensure correct monitoring of security conditions of infrastructure services that are necessary for data-in-process integrity, and avoidance of data leaks of relevant monitoring data.
Incremental certification

What?

- It is based on evidence acquired through accumulation of evidence regarding the satisfaction of security properties based on continuous monitoring.
- Should cover changes that may affect certified properties of cloud services without having to re-certify properties from scratch.

Why?

- Operational conditions within a cloud infrastructure may change.
- Cloud services and data may migrate to different cloud infrastructures within a cloud federation.
- Constituent services of composite services may be substituted (whether co-tenant or not).
Incremental certification – examples

- Re-validation of certificate due to changing operational conditions, e.g.:

  the certificate \( C \) for data integrity of a software service requires a certificate \( C' \) for the data isolation scheme operated by the cloud storage service;

  the software service migrates to a different node in a cloud federation \( \rightarrow \)

  \( C \) needs to be revalidated by considering whether the new hosting cloud has a certificate equivalent to (or appropriate substitute for) \( C' \)

- Use continuous monitoring to create new certificates or “strengthen” existing certificates with increased operational evidence, e.g.,

  The certificate of data-isolation for software service in a given infrastructure requires isolation of co-tenant services in the infrastructure; the certificate is continually validated through continuous monitoring of the infrastructure
New Certification models

- Need for
  New certification models to determine the evidence (type and extent) that needs to be considered to be able to certify a security property and how it will be used to assess the property

- Consequences
  Certification authorities sign “parametric” certificates, which are based on approved (signed) certification models, and may need to be validated (confirmed) dynamically
  →
  Changes in existing life cycle model of Issuing/Revocation
New Certification models (cont’d)

Certification models should address questions like:

- When two distinct pieces of evidence can be considered equivalent for a given security property?
- If conflicting evidence arises what happens to the certificate?
- Should a certificate be revalidated/revoked when:
  - The composition of a service changes
  - The deployment configuration of a service changes (e.g., code or data migration to another node in a federation)
  - The configuration of an infrastructure changes
- How certificate re-validation should be carried out? for example:
  - Could equivalent security properties be considered sufficient?
  - Could alternative equivalent pieces of evidence be used?
Interoperability & standards

- Interoperability with
  - emerging standards (e.g., GRC stack, STAR Registry) for cloud audit
  - reference cloud architectures (e.g., Nebula, CSA’s reference architecture)

- Contribution to standards, e.g.:
  - OCF (CSA; ongoing)
  - ISO 27017 (Cloud controls; ongoing)
  - ISO 27018 (Privacy in public clouds; ongoing)

- Key challenge/opportunity
  - Most of these standards are under development (e.g., OCF, ISO27017)
Where are we?

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

**Certification Infrastructure for Multi-Layer Cloud Services**

**THE CONTEXT**
Cloud technology offers a powerful approach to the provision of infrastructure, platforms and software services without incurring the considerable costs of owning, operating and maintaining the computational infrastructures required for this purpose.

**THE PROBLEM**
Despite its appeal from a cost perspective, cloud technology still raises concern regarding the security, privacy, governance and compliance of the data and software services offered through it. Such concerns arise from the difficulty to guarantee security properties of the different types of services available through clouds. Service providers are reluctant to take full responsibility of the security of their services once the services are uploaded and offered through a cloud. Also, cloud suppliers have historically refrained from accepting liability for security leaks. This reluctance stems from the fact that the provision and security of a cloud service is sensitive to changes due to cloud operation, as well as to potential interference between the features and behavior of all the site-dependent services in all layers of the cloud stack. Still many cloud users, including institutional ones, would like to rely on cloud-based services they use to exhibit certified security properties.

Brussels 18-19 Apr 2013
© G. Spanoudakis
Conclusions

- Cloud security still not perfect
- Security assessment: from audit to certification
- Focus on new certification models
  - Exploiting multiple types of evidence
  - Supporting increased automation, continuity and transparency
  - Close alignment with ongoing standardisation efforts