Security Service Level Agreement

Towards a fully provisioning of Security-as-a-Service


Prof. Valentina Casola
Università di Napoli Federico II
Italy
Outline

• Cloud Security Services Challenges:
  • Provide Security-as-a-Service
  • Security Service Level Agreements
  • Security SLA for an agile development

• Scientific Projects:
  – SPECS
  – MUSA
Key challenges

• **Security-as-a-Service**
  – Dynamically add/provide security capabilities even when services are offered by external CSP
• **Security Services and SLAs**
  – Security services delivered under the control of SLAs
• **Negotiating Security SLAs in Cloud?**
  – Enable users to negotiate per-user and per-service security SLAs in the Cloud
  – Enable providers to measure and guarantee SLOs
• **Monitoring Security SLAs in Cloud?**
  – Monitoring SLAs even when associated to services offered by external CSPs
Service Level Agreement (SLA)

• “Contract” which describes the Service, the associated quality levels and specifies the responsibilities (typically ‘soft’ formal obligations!) of both the Provider and the Customer.

Security? From SLA to Security SLA?
The SPECS Security SLA model

Negotiation is based on a Security SLA Template declaring all available
• **Resources**, providers
• **Security capabilities** (and related **security controls**)
• **Security metrics**

Requested guarantees are specified in form of (measurable) **SLOs**
Security SLA life cycle

Negotiate
• Agree on Security Controls and Metrics

Implement
• Activate Security Mechanism

Monitor
• Collect Security Metrics measurement

Remediate
• Identify Violations and apply remedies

Renegotiate
• Change SLA terms

TDW, 15 June 2016
Main concepts behind SLA negotiation

- Security SLA are modelled to cope with the semantic gap between not-expert customers and the needed standard technical controls that must be implemented to offer specific security capabilities
- The SLA model is compliant with available and on-going standards

Research challenges:
- The negotiation process must identify feasible offers to the customer
- The feasibility is evaluated according to security and CSP constraints
- The offers are evaluated according to the security level they provide
Main concepts behind SLA enforcement/remediation

• Dynamically add security to services even when services are provided by external CSP
  – Acquire and configure resources: SLA-based acquisition of resources and enforcement of security mechanisms

• Research challenges:
  – A quantitative approach to modular security to improve security of services/resources offered by External CSPs
  – Resource provision in a multi-cloud environment
  – Transparent adaptation of security services
Main concepts behind SLA monitoring

• Monitoring SLAs of services offered by external CSPs
  – Drive monitoring using SLAs
  – Notify possible SLA violations
  – Avoid violations with proactive reactions

• Research challenges:
  – Adapt monitoring to SLAs
  – Continuously monitor security of services offered by external CSPs
  – Measure the security (relationship with security SLO metrics) and incident management
SPECS: Secure provisioning of SLA-based secure services (FP7, 2014-2016)

SPECS framework provides APIs and tools to develop SPECS Application to let a target service be covered a SLA

- SPECS Applications available: CSP comparison, Secure WebPool, E2E encryption, ....

https://bitbucket.org/specs-team/

A security framework that includes:

- a) security-by-design mechanisms to allow application self-protection at runtime,
- b) methods and tools for the integrated security assurance in both the engineering and operation of multi-cloud applications
Conclusions

Security SLA for an agile development?

• **With Security SLA, we can effectively offer security as a service**

• Available security services, accessible and measurable, enable the development of new secure applications with a more agile approach

• **Standardization** activities: ISO/IEC 19086 (part 2 and part 4) on Cloud SLA metrics and Cloud SLA security and privacy
References and Contacts

www.specs-project.eu
https://bitbucket.org/specs-team/

www.musa-project.eu

NATRES and DPSP EU project clusters:
https://eucloudclusters.wordpress.com/