SWiN
BUR
* NE *

Computer
Science
&
Software
Engineering

An analysis of The Cloud Computing Security Problem

Mohamed Almorsy, John Grundy and Ingo Müller

Outline

- **Why we worry about security in the cloud?**
- **The cloud computing security problem**
- **Our observations**
- **A proposed approach for cloud computing security management.**

Why we worry about security in the Cloud?

- Enterprises outsource security control and management to a third party that hosts their IT assets (loss of control).

- Co-existence of assets of different tenants in the same location and using the same instance of the service.

- The lack of security guarantees in the SLAs between the cloud consumers and the cloud providers.

- Hosting this set of valuable assets on publicly available infrastructure increases the probability of attacks.

The cloud computing security problem (Existing Efforts)

- Cloud Security Alliance (CSA) and **The critical areas in cloud computing.**
  - Give a set of best practices but missed the existing problems and there relative causes.

- Meiko et al and **On Technical Security Issues in Cloud Computing**
  - Security issues related to XML-attcks, Brower attacks, and flooding attacks

- Subashini et al and **A survey on security issues in service delivery models of cloud computing**
  - **Each service delivery model with the exsiting security issues (Focused on SaaS)**

- Krešimir et al and **Cloud computing security issues and challenges**
  - List a set of security concerns in terms of questions that should be answered by community and the cloud providers

- Balachandra et al and **Cloud Security Issues**
  - SLA with focus on security SLAs

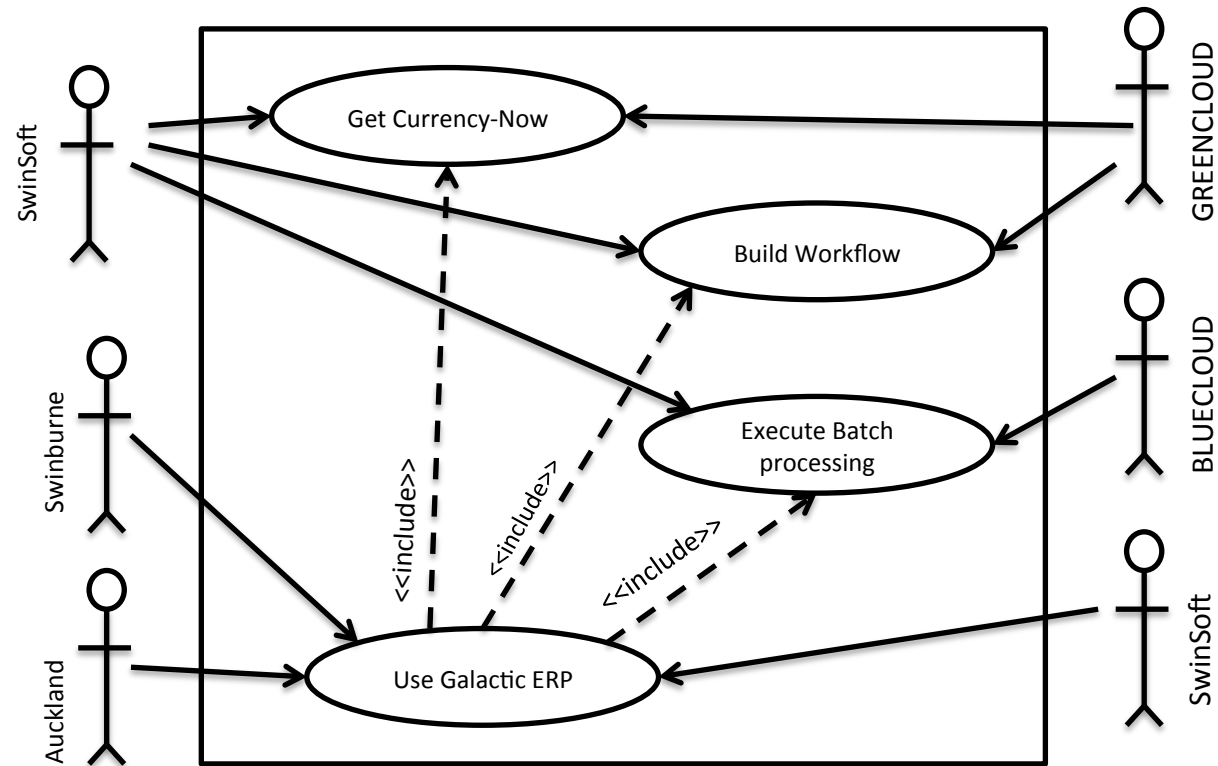# Cloud Computing security Problem (Proposed Approach)

| Analysis Dimension	Issues Found
Cloud Architecture	-Public clouds are more vulnerable to attacks -Different possible implementations of each service delivery models
Cloud Characteristics	-Multi-tenancy and Lack of Isolation - Location transparency and legal issues
Cloud Stakeholders	-Different security requirements should be enforced on a service instance. - Lack of security SLAs -Loss of control on the assets and the cloud platform
Cloud Dependency stack	-The long dependency stack and violation of lower layers. -Integration and coordination among BIG number of Sec Ctls.
Cloud Service Delivery Models	-IaaS security issues : virtualization -PaaS security issues: SOA related, APIs -SaaS security issues: Web applications' attacks & miss configs. -Cloud management layer: -Cloud access methods: Web Browsers, APIs, VPN,

Observations

Problem Domain	Solution domain
- The technology used (SOA, Virtualization) leads to a set of existing security problems	Focus on the problem abstraction, using model-based approaches
Multi-tenancy and isolation is a major dimension in the cloud security problem	Be inherent in the cloud architecture. Support for multi-tenancy and elasticity
Security management is very critical to control and manage this number of requirements and controls.	Support integration and coordination with other security controls. Be Adaptive

SaaS Level Motivating scenario

A proposed approach for cloud computing security management
High level architecture
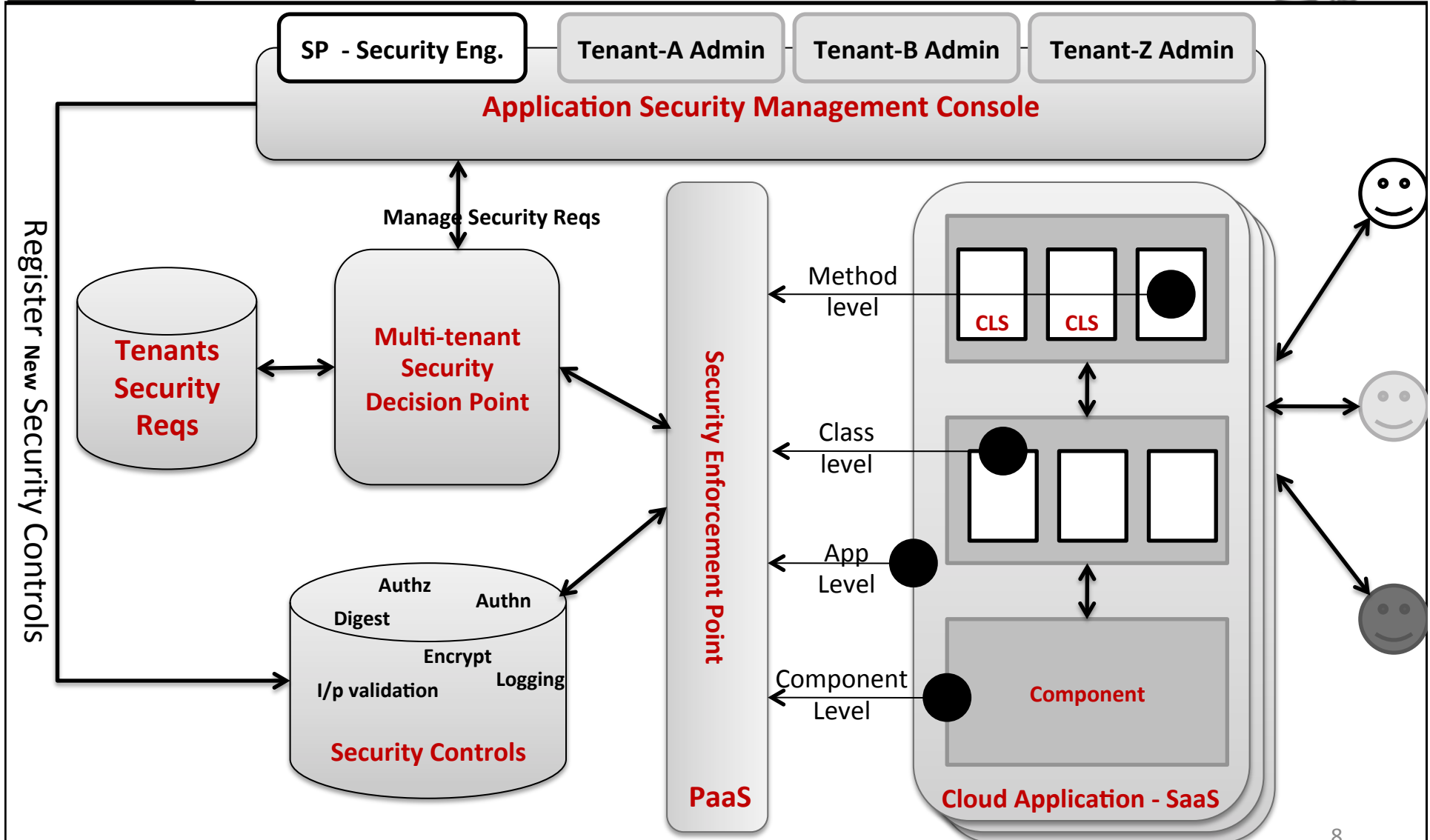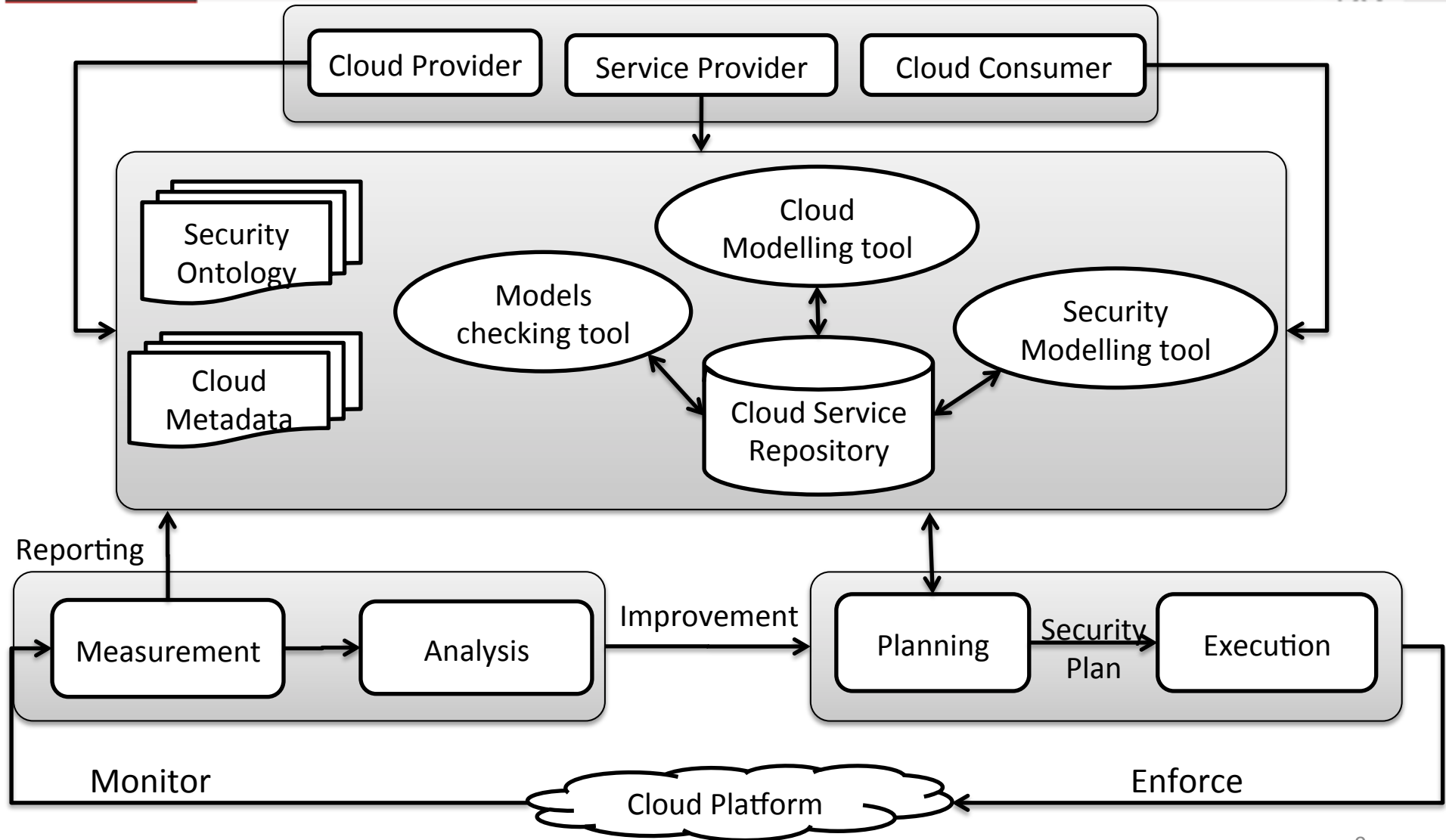
Q & A

Email: malmorsy@swin.edu.au
Phone: +61 3 9214 8699
Fax: +61 3 9819 0823
Office: EN403 – desk 32
Web page: Http://www.ict.swin.edu.au/ictstaff/malmorsy

References

- Almorsy, M., Grundy, J.C., and Mueller, I., An analysis of the cloud computing security problem, In Proceedings of the 2010 Asia Pacific Cloud Workshop 2010 (co-located with APSEC2010), Sydney, Nov 30 2010.
- Almorsy, M., Ibrahim, A., Grundy, J.C., Adaptive Security Management in SaaS Applications, Chapter 8 in Security, Privacy and Trust in Cloud Systems, Springer, 2013.
- Almorsy, M., Grundy, J.C. and Ibrahim, A., Automated Software Architecture Security Risk Analysis Using Formalized Signatures, 2013 IEEE/ACM International Conference on Software Engineering (ICSE 2013), San Franciso, May 2013, IEEE CS Press
- Almorsy, M., Grundy, J.C. and Ibrahim, A. Supporting Automated Vulnerability Analysis using Formalized Vulnerability Signatures, 27th IEEE/ACM International Conference on Automated Software Engineering (ASE 2012), Sept 3-7 2012, Essen, Germany, ACM Press.
- Almorsy, M., Grundy, J.C. and Ibrahim, A., Supporting Automated Software Re-Engineering Using "Re-Aspects", 27th IEEE/ACM International Conference on Automated Software Engineering (ASE 2012), Sept 3-7 2012, Essen, Germany, ACM Press.
- Almorsy, M., Grundy, J.C. and Ibrahim, I., VAM-aaS: Online Cloud Services Security Vulnerability Analysis and Mitigation-as-a-Service, 2012 International Conference on Web Information Systems Engineering (WISE 2012), Nov 28-30 2012, Paphos, Cyprus, LNCS, Springer.
- Almorsy, M., Grundy, J.C. and Ibrahim, A., MDSE@R: Model-Driven Security Engineering at Runtime, 4th International Symposium on Cyberspace Safety and Security (CSS 2012), Melbourne, Australia, Dec 12-13 2012, Springer.
- Almorsy, M., Grundy, J.C., Ibrahim, A., SMURF: Supporting Multi-tenancy Using Re-Aspects Framework, 17th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2012), Paris, France, July 2012, IEEE CS Press.
- Almorsy, M. and Grundy, J.C. TOSSMA: A Tenant-Oriented SaaS Security Management Architecture, 5th IEEE Conference on Cloud Computing (CLOUD 2012), IEEE CS Press, Waikiki, Hawai, USA, June 24-29 2012.