Security Assurance IN Service OuTSourcing (SAINTS)

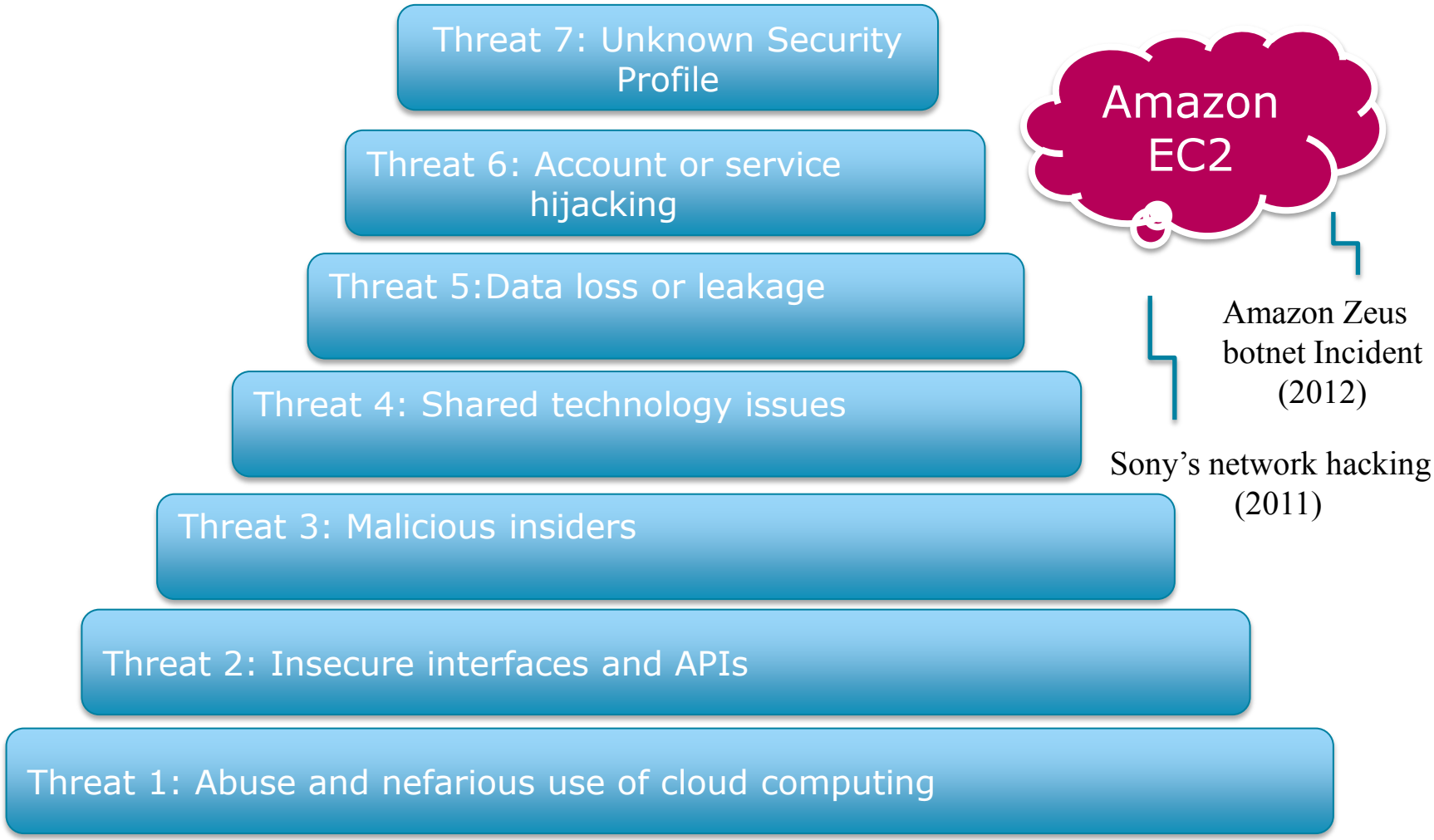
Moussa OUEDRAOGO, PhD

Service Science and Innovation, CRP Henri Tudor

Data centres and cloud services as the new trend for Businesses

- Advances have been made in the technology, particularly in networking and virtualisation.
- Outsourcing of competencies not core to the business
- Consumers are more interested in results rather than in the technical details
- Lesser management and maintenance cost

The Security Challenges of Sustaining the Momentum



From Security Concerns to Solutions

- Summary of the security challenges in cloud computing
  - Sensitive information are stored or processed by providers at geographically dispersed areas.
  - Security now lies in the hand of a third party
  - " …gracefully losing control while maintaining accountability" (Mell & Grance, 2009)

- The perspective solutions

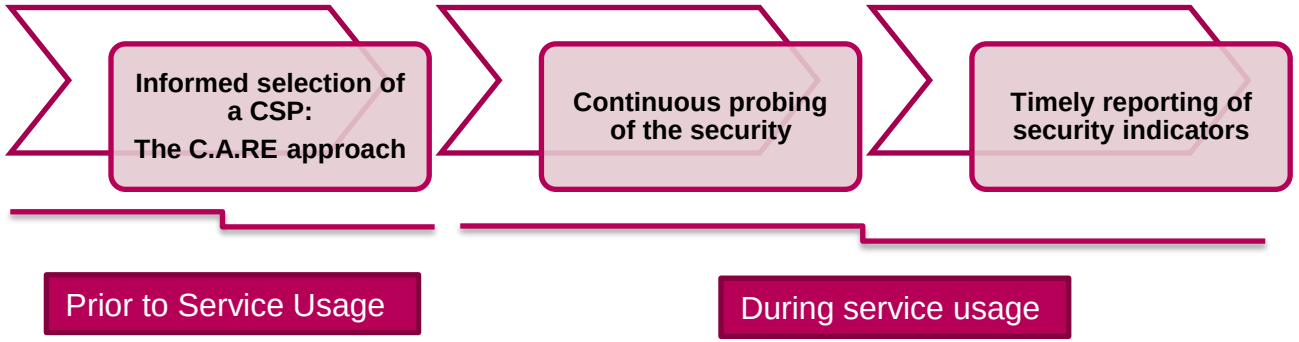
Threats affecting the wider adoption of the cloud	Type of security Concern	Related Security Solutions
Threat 2 and 6	VM security	Use of Trusted Cloud Computing Platform (TCCP), VM monitoring, encryption, encapsulation, abstraction
Threat 3-5	Data Security	Encryption, Access Control
Threat 7	Unknown security level	Security certification, Audits, SLA monitoring

  - blind trust between a provider and a consumer ?
  - Security Certification driven selection of the CSP?
  - …

- The missing links: Security transparency and mutual auditability (evidence based)

Filling the Gap: The SAINTS' Approach

- Establishing security transparency and mutual auditability in cloud services.



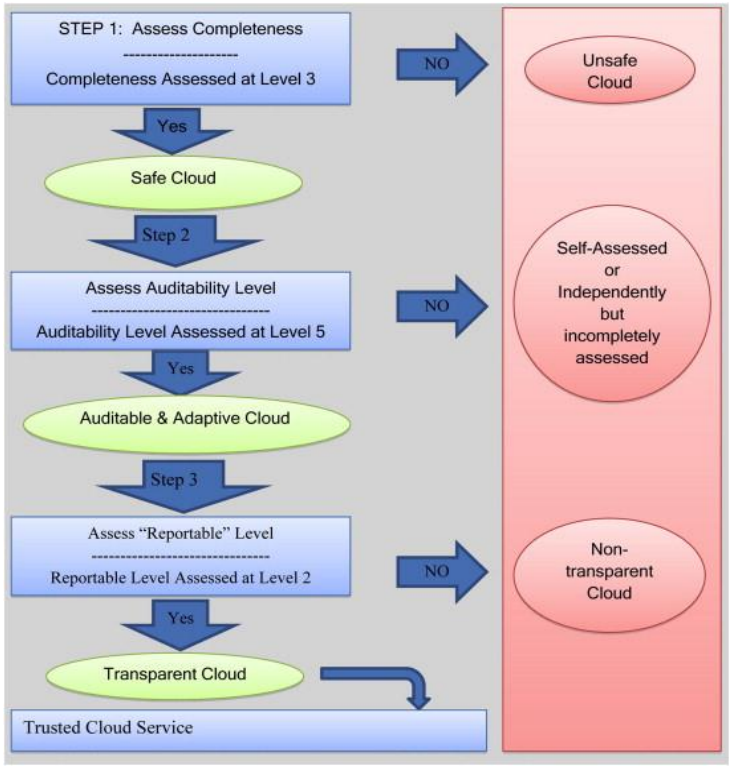
- Enable service providers (CSPs) to ensure their security is continuously aligned to increasingly strict regulatory requirements and also to consumers (CSCs)' service security needs.

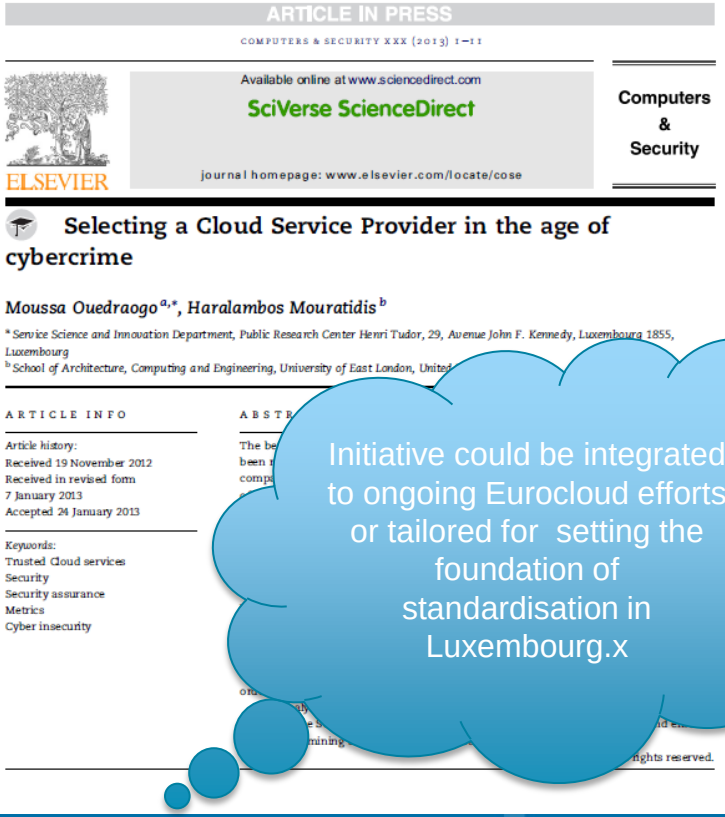
The C.A.RE Approach for Assessing and Ranking CSPs

Informed selection of a CSP: The C.A.RE approach

Continuous probing of the security

Timely reporting of security indicators





ARTICLE IN PRESS

COMPUTERS & SECURITY XXX (2013) 1–11

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

ELSEVIER

Selecting a Cloud Service Provider in the age of cybercrime

Moussa Ouedraogo [a,*], Haralambos Mouratidis [b]

[a] Service Science and Innovation Department, Public Research Center Henri Tudor, 29, Avenue John F. Kennedy, Luxembourg 1855, Luxembourg

[b] School of Architecture, Computing and Engineering, University of East London, United

ARTICLE INFO

Article history:
Received 19 November 2012
Received in revised form
7 January 2013
Accepted 24 January 2013

Keywords:
Trusted Cloud services
Security
Security assurance
Metrics
Cyber insecurity

ABSTR

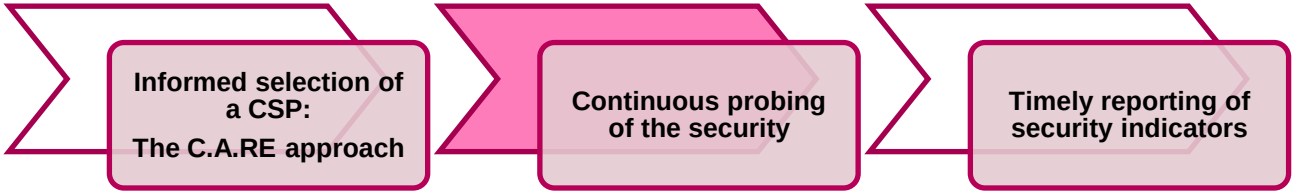
The be
been i
compa

mining

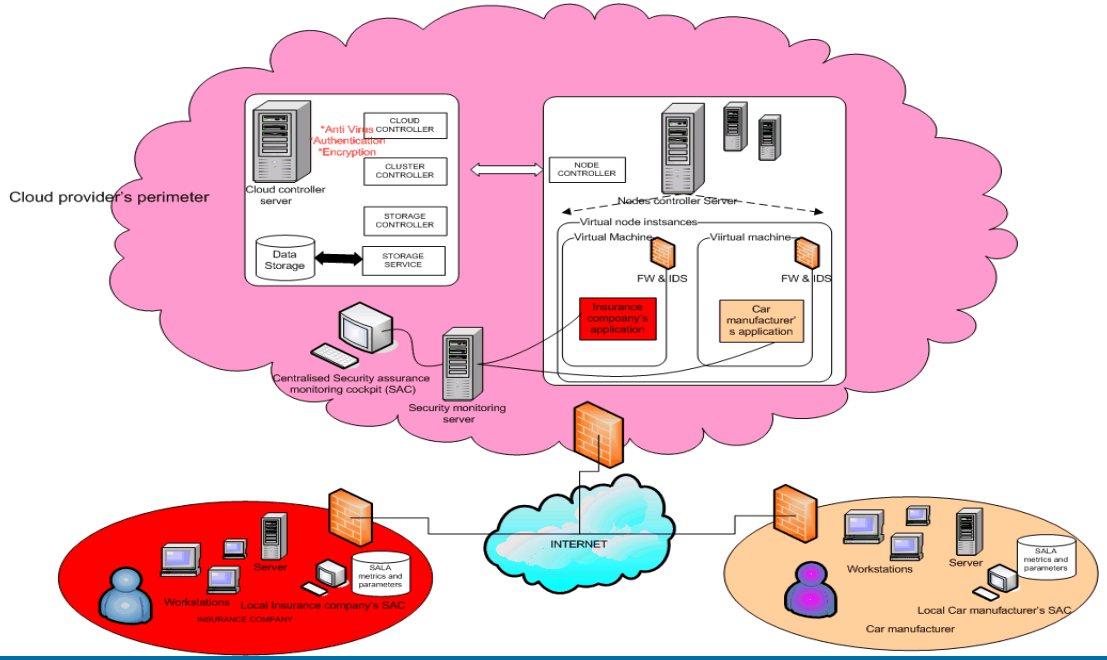
ights reserved.

Initiative could be integrated to ongoing Eurocloud efforts or tailored for setting the foundation of standardisation in Luxembourg.x

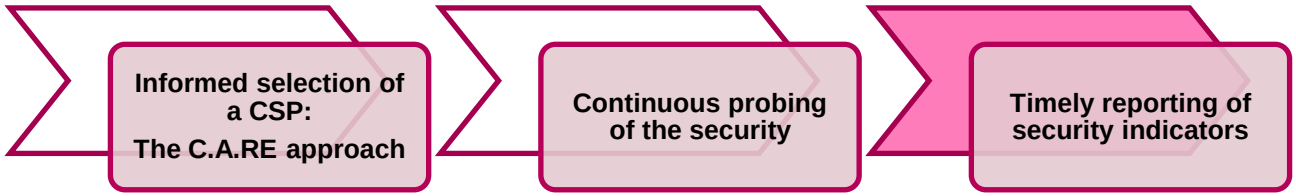
During the Usage Cloud Service: Continuous Probing of Security



- Develop a framework for enabling the appraisal and monitoring of the security assurance and their appropriate reporting to the provider and consumer
- Usage of a network of collaborative sofware sensors for anomalies detection.



During the Usage Service: Timely Reporting of Security Indicators



- Reporting of security indicators
  - Develop an architecture for enabling the exchange of security information
  - Determine relevant type of indicators for a CSC.
  - Prioritisation, correlation and aggregation of alerts.

Opinion of SMEs are sought for further elaborating the set of metrics that could be made available to the CSC.

Concluding Remarks

- Cloud services are being perceived as the ultimate solution for companies seeking to achieve both efficiency and cost cutting in the provisioning of services

- Cloud service as an "Old wine in new bottle" →a relatively good knowledge of the demons that come with it.
  - Security transparency and mutual auditability as the truly new security challenges, though scantly addressed in the literature and in practice.

- The SAINTS project purports to address such an issue through definition of techniques and a tool for:
  - Labeling and ranking CSPs based on their security offering, to enable an informed selection of a CSP by a CSC prior to embarking onto the cloud
  - Allowing CSC to continuously keep an eye on a security matter that is now devolved to the CSP

- Opinions from Actors in cloud services (CSCs and CSPs) are highly sought during the lifetime of the project.

tudor
PUBLIC RESEARCH CENTRE HENRI TUDOR

Thanking you for your time.

For further information, please contact:

Project Investigator: Moussa OUEDRAOGO

Email: moussa.ouedraogo@tudor.lu

Project Leader: Severine MIGNON

Email: severine.mignon@tudor.lu

Available for talk during Coffee Break!!