How can security requirements of critical Infrastructure IT shape Cloud Computing research?

Dr. Markus Tauber
markus.tauber@ait.ac.at
Austrian Institute of Technology (AIT)

25/04/2013

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

What do we mean when we say:

- Cloud
  - Private
  - Public
  - Semi-Hybrid
- Elasticity
- Scalability
- Critical Infrastructure
- Legal Requirements
  - EU data protection
  - SLA
- Cloud Behaviour
  - Resilience
  - Anomaly Detection
  - Security and Safety
- Cloudification

Problem Definition

- Everything goes cloud
  - Consumer data like our emails or photos (google mail and other google services)
  - Data base applications, especially when exposed to unpredictable load peaks
  - Governmental Data Centres peer with each other and create private clouds
  - Soon all kinds of applications (inc. CI) without us noticing it
  - ….
- Requirements for cloud applications vary
  - Commercial ones mainly to deal with load peaks and to get on-demand hardware resources (scalability & elasticity)
  - Requirements in CI regarding overall redundancy, data availability, authenticity, secure access are typically higher than in commercial applications.
- What is the problem?
  - Cloud services are per definition opaque and make it hard to determine reasons for failure and hence make the development of countermeasures hard
  - This also implies that it is hard to determine who's fault it is

CI in the Cloud

- Regulatory Issues
- Safety Issues (unlike other cloud services CI failure results in catastrophe, cascading effects)
- Security Issues
- Resilience Issues
- Legal Issues
  - EU Data Protection
  - Stringent Regulatory Requirements
  - Which data needs what level of protection
- Increased Awareness and visibility
- 7/24 availability
- Convergence of user concerns and CI priorities

Key Research Problems

- Provision of legal guidance for the use of technical information in matters of evidence and data protection as well as for SLA Management
- Novel Risk Management Approaches and Risk Metrics (inc. Catalogues) for CI in Cloud Environments
- Understanding Cloud Behaviour (monitoring, forensic analysis, anomaly detection, root cause analysis, resilience analysis in various layers)
- Best practise for secure cloud service implementation in CI (e.g evaluating methods like common criteria for cloudifying CI software)

The SECCRIT Project

- Why SECCRIT & why CI
  - Commercial focus more on elasticity & scalability
  - CI has higher interest in security aspects and redundancy
  - Commercial user requirements converge with CI regulatory requirements
  - Our output benefits the user and can be applied to commercial clouds as well
  - Highly user driven project including user and advisory board and real world demos

- What is SECCRIT
  - 10 Partners from Austria, Finland, Germany, Greece, Spain and the UK.
  - Project budget 4.8 Mio, partly funded by EC FP7 programme
  - Project duration 1.1.2013 – 31.12.2015

SEcure Cloud computing for CRitical Infrastructure IT

Contact

Dr. Markus Tauber
M +43 (0) 664 8251011
markus.tauber@ait.ac.at
Austrian Institute of Technology (AIT)
www.ait.ac.at/ict-security
www.seccrit.eu

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris