Methods and Technologies for Secure Cloud Computing for Critical InfrastructureIT

Dr Markus Tauber

SECCRIT Coordinator

AIT Austrian Institute of Technology

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

Why we are here

SEcure Cloud computing for CRitical infrastructure IT

- SECCRIT Introduction
- Technical & Legal Motivations
- Application of Research Outputs
- Increase the real-world implications via you

The SECCRIT Project

- Research project on secure Cloud Computing for critical infrastructure IT
- 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
- ~90% of the project completed
- 25 public deliverables

Critical Infrastructures go Cloud Computing

SEcure Cloud computing for CRitical infrastructure IT

Increasing Automation

Unpredictable Load-patterns

Increasing Amounts of Sensor Data

Require flexible compute and storage systems

SECCRIT's Overall Goal

analyse and evaluate cloud computing with respect to security risks in sensitive environments i.e. critical infrastructures

- Traffic Control
- Public Safety (CCTV)

to develop

- methodologies
- technologies,
- best practices for
  - secure,
  - trustworthy,
  - high assurance
  - legal compliant

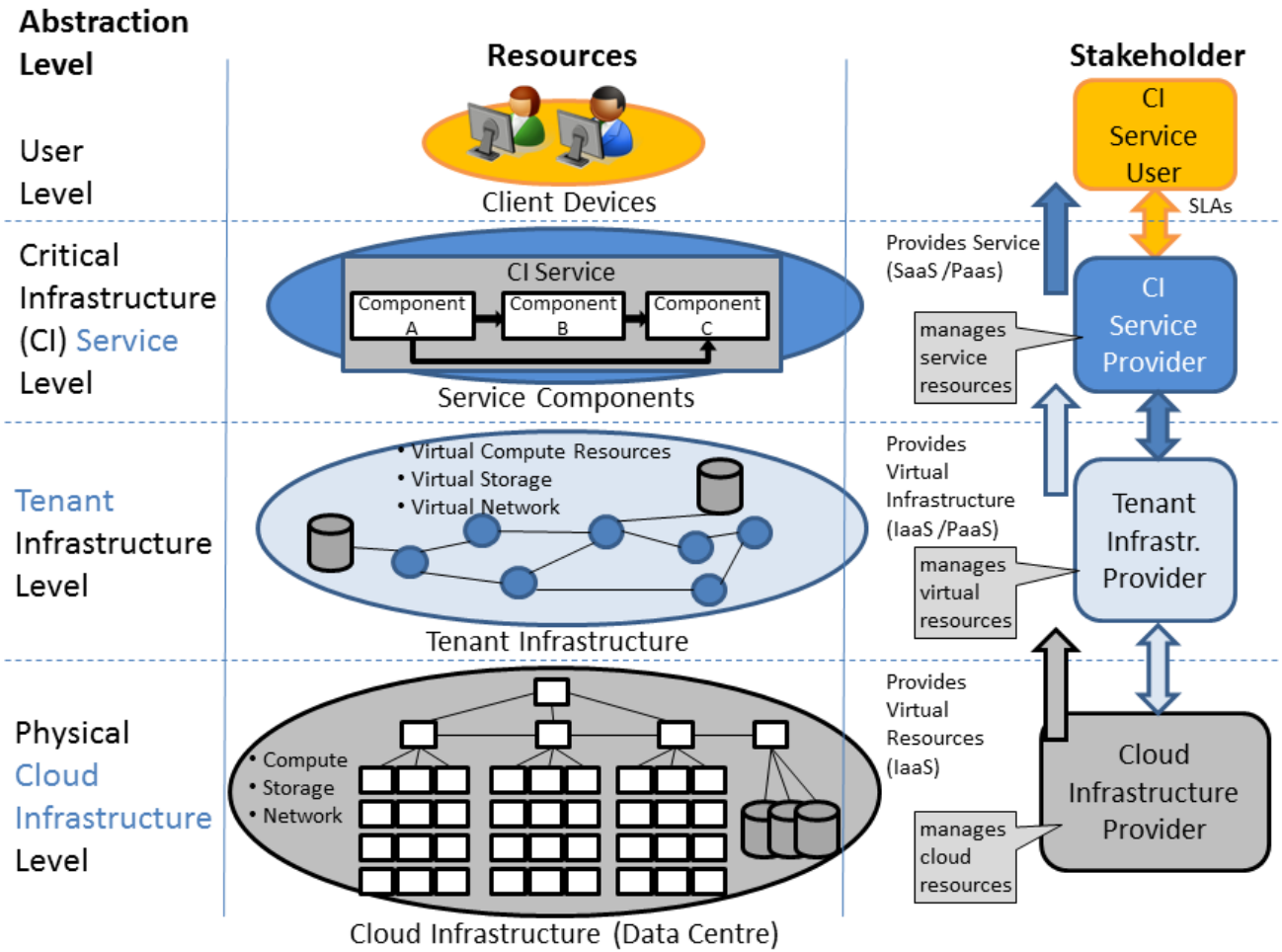
cloud computing environments for critical infrastructure IT.
Investigate real-world problems

Problem Definition – High Level

SEcure Cloud computing for CRitical infrastructure IT

- Everything goes cloud
  - Consumer data like our emails or photos (google mail and other google services)
  - Public administration IT services
  - Soon all kinds of applications (incl. Critical Infrastructure - CI)
- Requirements for cloud applications vary
  - Commercial applications mainly focus on scalability & elasticity
  - Requirements in CI regarding: overall redundancy, data availability, authenticity, secure access, trust and protection of the citizens are typically higher than in commercial applications.
  - Common Users Requirements converge with what is CI standard
- What is the problem?
  - Cloud services abstract over used resources, are opaque and make it hard to
    - determine **technical** reasons for (security) failure and hence make the
    - development of countermeasures
  - This also implies, from a **legal** perspective, that it is hard to
    - determine who's fault it is and
    - to show one hasn't acted negligent

Common Terminology - SECCRIT Architecture



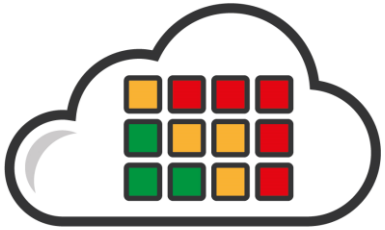
R. Bless, Flittner, M., Horneber, J., Hutchison, D., Jung, C., Pallas, F., Schöller, M., Shirazi, S. Noor ul Ha, Simpson, S., and Smith, P., "**Whitepaper** "AF 1.0" SECCRIT Architectural Framework". 2014. (and IEEE CloudCom)

SECCRIT Outputs

resilience framework including anomaly detection in the cloud

techno-legal guidance

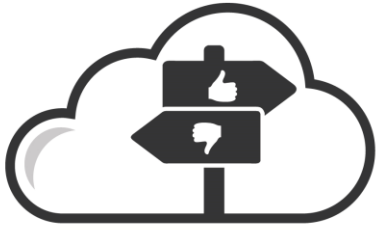
tools for audit trails and root cause analysis



risk assessment

policy specification, decision and enforcement

cloud assurance profile



model driven security guidelines

Demonstrator: Surveillance as a Service

The Subway Operator

The Security Service Provider

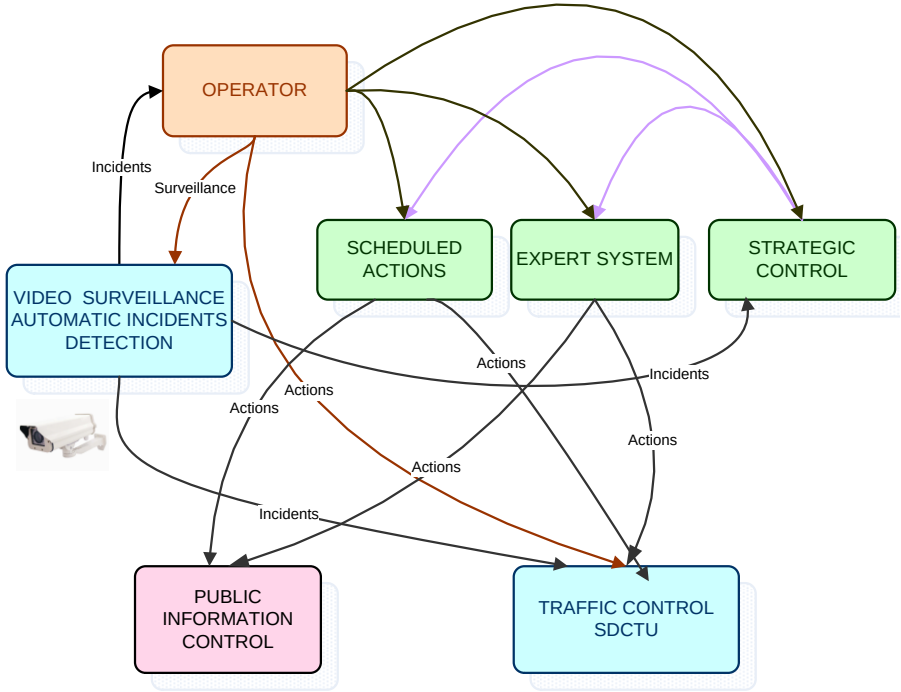
The Telecom Operator

The Tenant System Mgmt

The Cloud Mgmt Provider

Demonstrator: Traffic Control as a Service

- **Gather traffic data** from traffic sensors on the road
- Store traffic data in data bases
- Generate data and **reports about traffic status** and traffic evolution
- **Analyse** and relate the whole of **mobility data**
- Support to **define mobility polices** and traffic control strategies
- **Control traffic** on the road by Traffic Controllers, Traffic Ligths, Variable Messages Signals, etc.
- **Public transportation priority** by strategies like offering traffic lights priority



Execute traffic control strategies by operators manual actions or by automatic procedures.

Board Members, who support SECCRIT

E-Dataservices

GIP AG

Austrian Federal Ministry of Interior

Austrian Federal Ministry of Defense

The Austrian Federal Chancellery

GFT Technologies AG

State Library Denmark

SWK Stadtwerke Kaiserslautern GmbH

Younicos AG

More …..

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