Data protection versus storage efficiency and multi-tenancy

Dr. Ghassan Karame - NEC Laboratories - TREDISEC

Networking Session:

"Key challenges in end-to-end privacy/security in untrusted environments".

Cluster: Security and Trust. *ICT 2015* - Innovate, Connect, Transform

October 22nd 2015. Lisbon, Portugal

With the support of:

WISER
Wide-Impact cyber SEcurity Risk framework

The main problem

Top Threats Working Group

The Notorious Nine

Cloud Computing Top Threats in 2013

cloud security alliance®

To identify the top threats, CSA conducted a survey of industry experts to compile professional opinion on the greatest vulnerabilities within cloud computing. The Top Threats working group used these survey results alongside their expertise to craft the final 2013 report. The survey methodology validated that the threat listing reflects the most current concerns of the industry. In this most recent edition of this report, experts identified the following nine critical threats to cloud security (ranked in order of severity):

1. **Data Breaches**
2. **Data Loss**

There are a considerable number of security solutions for the cloud. However, most existing security technologies are not compatible with functional requirements of current clouds.

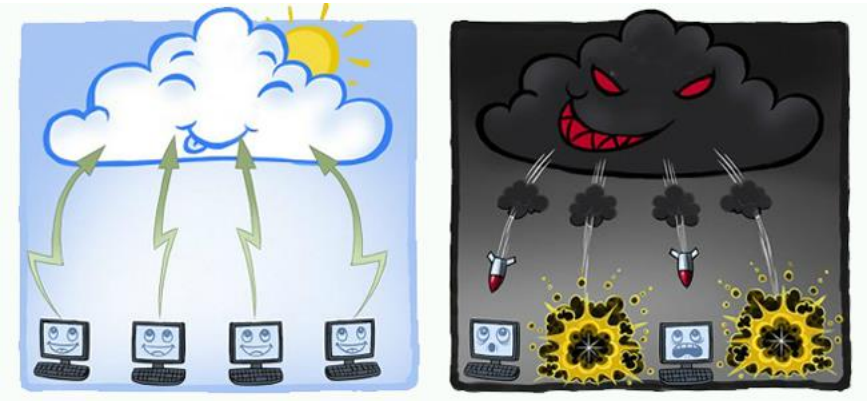
- **Multi-tenancy**
- **Storage efficiency**

"Key challenges in end-to-end privacy/security in untrusted environments"
ICT 2015 - Innovate, Connect, Transform. October 22nd 2015.

NEC

Current Challenges

- **Deduplication on encrypted multi-tenant data**.
  - Tenants do not trust each other, and might not share secret material.
- **Mechanisms to check the integrity and availability of multi-tenant data in presence of storage efficiency**.
  - Existing data auditing techniques have not been investigated over deduplicated data nor in multi-tenant settings.



Source: http://cdn.dejanseo.com.au/

- **Secure deletion of multi-tenant data in presence of deduplication**.
  - No solutions exists to ensure secure deletion in the presence of a malicious cloud.

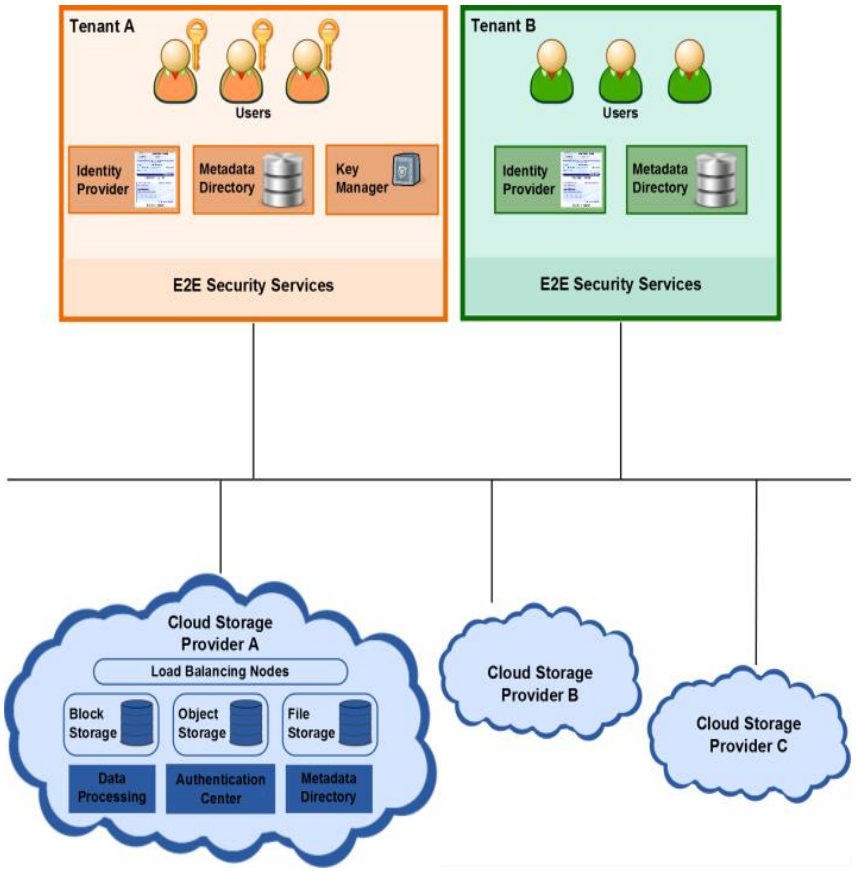
Current Challenges

- **Storage efficiency in presence of securely outsourced DBMS data.**
  - Data outsourcing schemes do not plug well with deduplication and compression techniques.
- **Secure outsourced analytics/processing in a multi-tenant environment.**
  - Not easy to outsource data and computations by mistrusting tenants such that privacy-processing over this data is efficiently realized.

- **Distributed enforcement of access control policies.**
  - How to enforce access control in existing clouds amongst mistrusting tenants?

Expected Results

- **Designing novel end-to-end security solutions to reconcile conflicting functional and security requirements**
  - **Supporting data reduction**
  - **Enabling secure data processing**
  - **Enhancing data availability and integrity**
  - **Ensuring user isolation in multi-tenant systems**



Ideas for the future

- **All the proposed features should be included as part of a unique architecture**.
  - This requires a delicate design of the various system components in order to prevent any possible incompatibilities that might arise between them.
- **The aim is to foster the concepts of "security and privacy by design"**.
  - This will **provide strong incentives for small and medium businesses** to reduce their costs and securely store and process their outsourced data in the cloud.

Further information:

- Name: **Ghassan Karame, NEC Laboratories Europe**
- Email: **ghassan.karame@neclab.eu**

- Project website: **http://www.tredisec.eu/**

We would love to hear from you!

Please fill in the form any questions you might have and we will get back to you by email asap.

NEC

tredisec