PRISMACLOUD

Cloud Security and Privacy by Design
Horizon 2020 programme; duration 2/2015-7/2018

—

6th International Conference on eDemocracy
Citizen rights in the world of the new computing paradigms

Thomas Länger

thomas.laenger@unil.ch
Swiss Cybersecurity Advisory & Research Group
Université de Lausanne

10 Dec 2015 – 16:15-17:15

UNIL | Université de Lausanne

Talk outline

- Present H2020 project **PRISMACLOUD** (2.2015 - 8.2018) (Abbr.: Privacy and Security Maintaining Services in the Cloud)
- Current cloud computing models
- Cloud market and cloud providers
- Governance in cloud computing
- More organisational and technical risks
- PRISMACLOUD approach and portfolio

...on 17 slides

Definition of cloud computing

Widely accepted definition by the NIST (Special Publication SP800-145, 7 pages; **emph.** by me):

> *Cloud computing is a model for enabling* **ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources** *(e.g., networks, servers, storage, applications, and services) that can be* **rapidly provisioned and released with minimal management effort or service provider interaction***. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

Definition of cloud computing

Widely accepted definition by the NIST (Special Publication SP800-145, 7 pages; **emph.** by me):

> *Cloud computing is a model for enabling* **ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources** *(e.g., networks, servers, storage, applications, and services) that can be* **rapidly provisioned and released with minimal management effort or service provider interaction***. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

Sounds like an end-user paradise. But is it really true?

UNIL | Université de Lausanne

This cloud model is composed of...

five essential characteristics:

- On-demand self-**service**, Broad network access
- Resource pooling, Rapid elasticity, Measured **service**

three service models:

- Software as a **service** (SaaS), Platform as a **service** (PaaS)
- Infrastructure as a **service** (IaaS), + data storage-, hardware-,
- function-, big data-, security-, management- **as a service**

four deployment models:

- Private cloud, Community cloud
- Public cloud, Hybrid cloud (all SP800-145)

UNIL | Université de Lausanne

"Servicification" - transform a product into a service

We witness now the **servicification or tertiarisation** of the ICT sector:

- The ICT products are enrolled to a greater extent to cloud providers, instead as to end-users;
- end users only need to provide an access platform (e.g. a thin client with a web browser) and an online connection;
- The cloud providers generate the additional value of the services and sell the services to the end-users;
- the cloud providers **get access** to valuable data and metadata; cloud providers **control access** to the data.

UNIL | Université de Lausanne

Cloud market: A few figures

Management consulter Accenture sees 46% of the IT spending for 'cloud-related platforms and applications' by 2016

> *A Cloud Computing Forecast Summary for 2013 - 2017 from IDC, Gartner and KPMG; online: www.prweb.com/releases/2013/11/prweb11341594.htm, citing a study by Accenture (2013)*

The cloud computing market is by 2015 estimated to be in the region of USD 150 billion, and will probably grow by the year 2018 to around USD 200 billion

> *Transparency Market Research: Cloud Computing Services Market - Global Industry Size, Share, Trends, Analysis And Forecasts 2012 - 2018, online: www.transparencymarketresearch.com/cloud-computing-services-market.html*

"Amazon Web Services is a $5 billion business and still growing fast"

> *Amazon quaterly earnings report Q1/2015 phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-newsArticle&ID=20395989*

The clouds: who provides them?

The **cloud service providers** are well known from their past in IT:

- Amazon Web Services (biggest retailer, biggest cloud provider)
- Google-YouTube-Android: (bought 181 companies 2001-2015)
- Microsoft-Azure-Skype,
- Facebook (bought 53 companies 2005-2015) etc. etc.

Some of them also want to **'get a grip' on the data** or at least on the meta-data. Most public clouds reserve themselves access to

- who communicates with whom,
- and when, and where from (all these are metadata);
- establish detailed profiles of millions of individuals and dragnet or mine them for valuable information,
- identify potential 'targets' for marketing

Governance

For **sensitive data**, like data in **critical infrastructures**, or private **personal data (e.g. health data)**, European legislation does not only reserve **ultimate control of the data to its owner** (which is in the case of the health case the patient), but also requires **data confidentiality for extended periods of time** (like 80 years into the future).

On the other hands, companies **move data between jurisdictions** and such prevent the enforcement of legal rights. Big corporations use loop-holes in legal systems and influence policy processes by extensive lobbying.

More pending risks in cloud computing

As the **cloud metaphor** already indicates, **you put your data into some opaque thing** somewhere on the internet. But that's just what you wanted to do: Give the data to somebody else for taking care of it. This is may be quite practical, and save you some money in the first place (see the advantages listed in NIST definition), but **leads to a series of information risks**:

- Policy and organisational risks
  - lack of control, lack of information on processing
  - loss of governance (data moved to another legislation)
  - vendor lock in
- Technical risks
  - diverse data protection risks
  - isolation failure
  - data loss, abuse, malicious outsider and insider etc.

UNIL | Université de Lausanne

Horizon 2020 project PRISMACLOUD approach

A 3.5 year project with the goal to **enable end-to-end security for cloud users**, and to provide tools to **reinstate governance to end users** with the best technical means – **by cryptography**

- Provide 10 cryptographic functions to support end user goals in cloud computing from the following 4 fields:
  - Protection of data at rest
  - More privacy of end users
  - Authentication of stored and processed data
  - Certification of virtual infrastructures
- Make cryptography available, usable and economically relevant for clouds – and build it into systems by design
- Evaluate its capabilities in real-life scenarios
- Put a focus on usability, policy, and standardisation

UNIL | Université de Lausanne

Example: Secure cloud storage "by default"

Provide a storage service **as most users would expect:**

- the data remains **strongly confidential**
- the data is readily **available on demand**
- the data may **easily be shared** with others
- the data can easily be transferred to another provider **when the user wants to**

Solution: use a **cryptographic storage network**

- use an information dispersal algorithm with a threshold scheme (Shamir secret sharing, e.g. 3 out of 5)
- "keyless encryption" under non-collusion assumption
- capable of long term security (substitution of shares to counter collusion threat)
- implicit backup
- change of provider: (take a provider's share out of the set, generate a new share for the new provider)

Services enabled by PRISMACLOUD crypto tools (Part I)

- **Data storage in the cloud**
- Secure cloud storage "by default"
  - enabled by: Cryptographic storage network
- Moving a legacy application to the cloud
  - enabled by: Data security for database applications
- **User privacy protection**
- Non-identifiable and untrackable use of a cloud service
- Minimal exposure of personal data during authentication
  - enabled by: Anonymous credentials and Group signatures

Services enabled by PRISMACLOUD crypto tools (Part II)

- **Authentication of stored and processed data**
- Black out information from electronically signed documents
- Allow someone to modify your electronically signed documents
  - enabled by: Malleable signtures
- Controlling the correctness of delegated computations
  - enabled by: Verifiable computation
- **Certification of virtualised infrastructures**:
  - Certification of virtualised infrastructures

H2020 Project PrismaCloud

- Call: H2020-ICT-2014-1
- Acronym: PRISMACLOUD
- Type of Action: RIA
- Number: 644962
- Partners: 16
- Duration: 42 months
- Start Date: 2015-02-01
- Estimated Project Cost: 8.5M€
- Requested EU Contrib.: 8M€
- Coordinator: Austrian Institute of Technology GmbH
- **www.prismacloud.eu**

Unil
UNIL | Université de Lausanne

PRISMACLOUD Partners

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

KARLSTADS UNIVERSITET

cea leti

etra I+D

Newcastle University

Rechteckiges Ausschneiden

Atos

FC SR
Fondazione
Centro San Raffaele

IBM

Unil
UNIL | Université de Lausanne

interoute
from the ground to the cloud

LOMBARDIA INFORMATICA

MP
MIKROPLAN

IAIK TU Graz

UNIVERSITÄT PASSAU

XITRUST
SECURE TECHNOLOGIES

TECHNISCHE UNIVERSITÄT DARMSTADT

Newcastle University
TECHNISCHE UNIVERSITÄT DARMSTADT
MP MIKROPLAN
UNIVERSITÄT PASSAU
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
IAIK TU Graz
cea
Atos
etra I+D
XITRUST
Unil UNIL | Université de Lausanne
interoute
SR
LOMBARDIA INFORMATICA
IBM
ISRAEL

ıne

About: Thomas Länger

Hi, I'm post-doc researcher at the **Swiss Cybersecurity Advisory & Research Group** of the Institute of Information Systems, Faculty of Business and Economics, University of Lausanne.

Currently active in H2020 Project "PrismaCloud" 1 Feb 2015 + 42 month; 16 Partners, Project cost approx. 8.5M€ "Develop next-generation cryptographically secured services for the cloud."
My tasks: cloud computing (cc) security design patterns; cc standardisation; end user impact analysis of cc.

UNIL | Université de Lausanne