MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

IN COLLABORATION WITH MIT MANAGEMENT SLOAN SCHOOL

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

MASTER MEIM 2022-2023

Security Issues in Cloud Computing

PART ONE - INTRODUCTION

Luigi CATUOGNO, PhD

Associate Professor in Computer Science at Università degli Studi di Napoli Parthenope (ITALY)

1

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Security Issues in Cloud Computing

Since its appearance, Cloud Computing has found fitting applications in numerous scenarios.

Nevertheless, the Cloud Computing paradigm challenges many amongst the most established techniques, practices and beliefs related to security in distributed systems.

2

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Security Issues in Cloud Computing

First, the `Cloud' enriches ICT ecosystems introducing news parties, entities and models of interaction.

In such ecosystems, tasks are accomplished, and services are provided by means of the cooperation among different (and independent) parties.

Entities and relationships may vary over time depending on needs, the appearance of new models, the introduction of new services…

3

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Security Issues in Cloud Computing

Second, Cloud Computing dramatically changes the perspective of security.

The Cloud must provide a safe playground where the ability of individual players to exploit resources illegitimately and harm each other is limited

In the Cloud, there are no well marked `boundaries' between inside and outside to be defended: “friends” and “enemies” coexist in the same environment

4

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Security Issues in Cloud Computing

This requires the security infrastructure design takes in account that requirements raised by different stakeholders (sometimes conflicting), must be met without imposing strong limitations to the overall system operation.

The goal is establishing trust in interaction among partners instead of isolating them from each other.

5

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Security Issues in Cloud Computing

In the following we provide an overview of the main security issues and requirement raised in the Cloud scenario, along with the main techniques and tools that are nowadays on the shelf to cope with them.

6

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Summary

Let's start with an example: How Cloud Computing Changes Security

We will see that with respect to «Traditional Security»:

- Cloud Security is approached from new points of view;
- Cloud Computing brings new threats

7

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Summary

Concerns with Cloud Security:

Which aspects of Cloud ecosystems are considered more threatening by customers?

- Loss of control?, Lack of trust? Multi-tenancy?

8

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Summary

Cloud security: Challanges

How the cloud computing paradigm impacts on data security:

- Confidentiality, Integrity, Availability, Privacy, Regulatory compliance
- How Cloud Computing increases the attack surface

9

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Summary

Towards possible solutions:

Some approaches to minimize:

- loss of control and lack of trust

And;

- Governing multi-tenancy

10

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Let's take an example

HOW CLOUD COMPUTING CHANGES SECURITY PERSPECTIVES

11

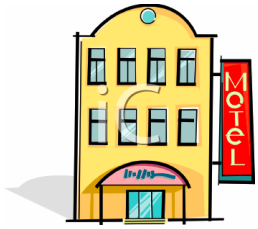
MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Traditional vs Cloud Security

Clouds change the approach to security. It is like passing from securing a house to secure a motel

HOUSE



MOTEL

Many things change… priorities, points of view…

A great example by Ragib Hasan, `http://ragibhasan.com`

12

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

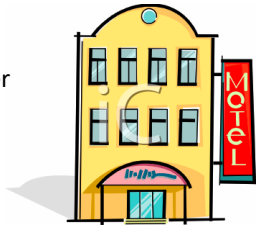
UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Traditional vs Cloud Security

Clouds change the approach to security. It is like passing from securing a house to secure a motel

HOUSE

The owner and the user are the same person.



MOTEL

The owner rents his rooms to different tenants (users)

Tenants share common facilities (stairs, elevator…)

Many things change… priorities, points of view…

A great example by Ragib Hasan, http://ragibhasan.com

13

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Traditional vs Cloud Security

Clouds change the approach to security. It is like passing from securing a house to secure a motel

HOUSE

- Securing perimeter
- Checking for intruders
- Securing assets
- …

MOTEL

Securing each room against:

- The bad guy in the next room
- Dishonest staff membners
- …

Many things change… priorities, points of view…

A great example by Ragib Hasan, http://ragibhasan.com

14

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Traditional vs Cloud Security

In traditional systems

Everything to be protected is within the walls

Security measures mostly aim at keeping bad guys out

The attacker need to either compromise the auth/access control system or impersonate existing users

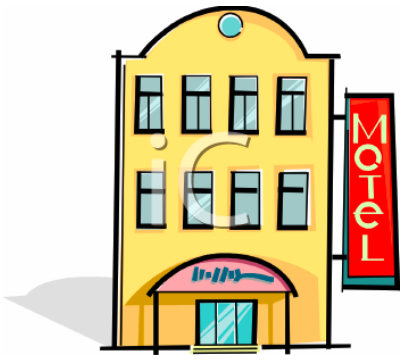
A great example by Ragib Hasan, **http://ragibhasan.com**

15

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Traditional vs Cloud Security



The cloud is shared by muliple *autonomous* users

Malicious users legitimately access the same infrastructure of their potential victims

Attacking other users from inside is often easier

Adversaries can take advantage of sharing the same infrastructure with their victims

A great example by Ragib Hasan, **http://ragibhasan.com**

16

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Concerns with Cloud security…

17

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Concerns with Cloud security…

Most concerns with Cloud security raise from:

- Loss of control
- Lack of trust
- Multi-tenancy drawbacks

Anyway, these problems are common to the majority of 3rd party management models

18

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Loss of control

Consumer's loss of control

- Data, application, resources are located with the provider's
- User identity management is handled by the cloud
- User's resources access control rules, security policies and enforcement are managed by the cloud provider

19

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Loss of control

Consumer relies on provider to ensure

- Data security and privacy
- Resource availability
- Monitoring and repairing of services/resources

20

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Lack of trust

Trusting third parties requires taking risks

- Defining trust and risk: *«the opposite sides of the same coin»*
- Establishing roles, responsibilities and guarantees
- Defining metrics
- Defunct third party management schemes

21

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Multi-tenancy drawbacks

Conflict between tenants sharing the same pool of resources

- Every tenant pursues the best resorce assignment regardless the needs of the others

How does multi-tenancy deal with conflict of interest

- Making tenants to agree on a common resource request/release policy?
- Isolating tenants, so that resource usage of each does not affects the others performace
  - How to provide separation between tenants?

22

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Multi-tenancy drawbacks

Multi-tenancy brings a new threat (Side Channel Attack):

An attacker can take advantage of sharing the same physical/logical infrastructure with its potential victim

- Gathering private information by taking *indirect orbservations*
- Affecting/compromising the victims's *payload* operation by stressing their common resource pools

23

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Concerns with Cloud security…

Concerns related to: loss of control, lack of trust, multi-tenancy… considerably challange every aspect of security:

- Confidentiality
- Integrity
- Availability
- Privacy
- Vulnerability
- Regulatory compliance

24

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Cloud Security challenges

25

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Confidentiality

How to:

- ensure that sensitive data stored on a cloud remain confidential?
- prevent Cloud compromises from ending up leaking confidential client data?
- guarentee cloud provider itself be honest and won't peek into the data?

26

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Integrity

How to:

- verify that the cloud provider is doing the computations correctly?
- verify that data has not be corrupted/lost?
- ensure that the cloud provider really stored clients' data without tampering with it?

27

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Availability

How to:

- Ensure that user data «is still there»? *(proof-of-retrievability)*
- Ensure that the cloud scale well-enough?

What if:

- the cloud provider is attacked in a DoS attack?
- the cloud provider goes out of business?

28

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Privacy

The cloud is able to observe the behavior and the activity of its users for a long time

Even without peeking through their data, the Cloud provider can learn a lot of potentially sensitive information about them

- How to prevent the Cloud to run data mining algorithms to get large amounts of information on clients?

29

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Increased attack surface

Entity outside the organization now stores and computes data and so

- Attackers can now target the communication link between cloud provider and clients
- Cloud provider employees can be phished
- …

30

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Regulatory Compliance

Auditability and forensics (out of control of data)

- Difficult to audit data held outside organization in a cloud
- Forensics also mad difficult since now clients don't maintain locally

Legal dilemma and transitive trust issues

- Who is responsible for complying with regulations? (e.g. SOX, HIPAA, GDPR?)
- If cloud provider subcontracts to third party clouds, will the data still be secure?

31

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Possible solutions

32

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Monitoring

Cloud consumer needs situational awareness for critical applications

- When underlying components fail, what is the effect of the failure to the mission logic?
- What recovery measures can be take?
  - By whom (provider, consumer)?

33

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Monitoring

Provide mechanisms that enable the provider to act on attacks he can handle

- Infrastructure remapping
  - Create new or move existing fault domains
- Shutting down offending components or targets
  - And assigning tenants with porting if necessary
- repairs

34

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Monitoring

Provide mechanisms that enable the consumer to act on attacks he can handle

- Application-level monitoring
- RAdAC (Risk-adaptable Access Control)
- VM porting wiht remote attestation of target physical host
- Provide ability to move the user's application to another cloud

35

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Use different CSPs

Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture in which:

- Spread the risk
- Increase redundancy (per-task or per-application)
- Increase chanche of mission completion for critical applications

36

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Use different CSPs

Possible issues to consider:

- Policy incompatibility
- Data dependency between clouds
- Differing data semantics across clouds
  - Monitoring technologies
- It is worth to spread your sensitive data across multiple clouds?
  - Redundancy could increase risk of exposure

37

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Access Control

Many possible layers of access control

- E.g. Access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs. And access to objects within a VM
- Depending on the deployment model used, some of these will be controlled by the provider and others by the consumer

38

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Access Control

Regardless of deployment model, provider needs to manage the user authentication and access control procedures (to the cloud)

- Federated Identity Management: access control management burden still lies with the provider
- Requires user to place a large amount of trusto on the provider in terms of security, management and maintenance of access control policies

39

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Loss of Control: Access Control

Consumer-managed access control

- Consumer retains decision-making process to retain some control, requiring less trust of the provider
- Requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decision between the cloud provider and consumer
  - It also needs to be able to guarantee that the provider will uphold the consumer-side's access decision
- Should be at least as secure as the traditional access control model

40

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Lack of Trust: policy language

Consumers have specific security needs but don't have a say-so in how they are handled

- Currently consumers cannot dictate their requirements to the providers (SLAs are one-sided)

41

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Lack of Trust: policy language

Standard language to convey one's policies and expectations

- Agreed upon and upheld by both sides
- Standard Language for representing SLAs

Create policy language with the following characteristics:

- Machine-understandable (or at least processable)
- Easy to combine/merge and compare

42

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Lack of Trust: certification

Certification

- Some form of reputable, independent, comparable assessment and description of security feature and assurance

Risk Assessment

- Performed by certified third parties
- Provides consumers with additional assurance

43

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Multi-tenancy drawbacks

Can't really force the provider to accept less tenants

Can try to increase isolation between tenants

- Strong isolation techniques
- QoS requirements need to be met
- Policy specification

44

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Minimize Multi-tenancy drawbacks

Can try to increase trust in the tenants

- Who is the insider? where is the security boundary? Who can I trust?
- Use SLAs to enforce trusted behavior

45

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Conclusion

Cloud Computing is sometimes viewed as a reincarnation of the classic mainframe client-server model

- However, resources are ubiquitous, scalable, highly virtualized
- Contains all the traditional threats, as well as new ones

46

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Conclusion

In developing solutions to cloud computing secuirty issues it may be helpful to identify the problems and approaches in terms of

- Loss of control
- Lack of trust
- Multi-tenancy problems

47

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

IN COLLABORATION WITH MIT MANAGEMENT SLOAN SCHOOL

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

MASTER MEIM 2022-2023

Thank you!

48