Fraud Threats Disclosure through Cloud Information Security Framework

Theodoros Mavroeidakos[1,2] and Dimitrios D. Vergados[2]

[1]School of Electrical and Computer Engineering
National Technical University of Athens, Greece
Email: el10807@central.ntua.gr

[2]Department of Informatics
University of Piraeus, Greece
Email: vergados@unipi.gr

UNIVERSITY OF PIRAEUS RESEARCH CENTER

Outline

Introduction

What's the situation with fraud on CC environments?

- According to International Vice President of ISACA, Jeff Spivey:
  - *"All of the advantages of the cloud for enterprises are [also] the advantages for the bad guys."*
  - *"It is the anonymity and scale that is attractive to the fraudsters."*
- The CC characteristics, such as rapid elasticity, on-demand provisioning and pay-as-you-go model of pricing, are all as appealing to fraudsters as to ordinary users.
- Cloud-based services are characterized as high-risk due to: *weak authentication schemes and ineffective access control allowing anonymous access to CC resources.*

Motivation

This work aims at encountering fraud threats on CC environments through a Cloud Information Security Framework.

- Its main **objectives** are to:
  - address fraud issues and challenges both in the functional as well as the technical layer of the CC environment,
  - define the necessary cyberspace operations which shall be implemented so as to achieve a high level of security prior to the adaptation of processes and activities aiming to mitigate fraud threats,
  - achieve governance control over internal corporate actions which are performed on the collected data and any contextual information,
  - facilitate analysis about regulatory and legal compliance in conjunction with emerging constrains.

Related Work

Most studies have only focused on methods and frameworks to accomplish security or fraud threats mitigation independently.

- European Network and Information Security Agency (ENISA) examines Critical Information Infrastructure Protection (CIIP) issues by analyzing the effects of cyber-attacks at the end-service [4].
- ENISA proposes in [5], a security framework which is modeled in four phases in order to facilitate the adoption of the CC paradigm by governments of the Member States of the European Union (EU).
  - This framework is based on the Plan-Do-Check-Act (PDCA) cycle so as to organize and manage the security objectives.
- The National Institute of Standards and Technology (NIST) proposes guidelines on security and privacy in public cloud computing in [6].

Related Work

- NIST fills the gap between the available security standards and the security categories which shall be addressed in the context of a protected CC environment [7]. of cyber-attacks at the end-service [4].
- Moreover, NIST presents the Cloud Computing Security Reference Architecture (NCC-SRA) which defines a predictive model in order to secure the NISTs Cloud Computing [8]. Architecture.
  - This report introduces a methodology for applying a Cloud-adapted Risk Management Framework divided in specific steps using a set of security components so as to engineer a protected CC environment.
- NIST also introduces [9] security and privacy controls so as to construct resilient environments against cyber threats in federal CC environments.

Related Work

- Hormozi et al. argue in [10] that the detection of fraudulent activities on CC environments shall be performed by an Artificial Immune System (AIS) based on the Negative Selection Algorithm (NSA)
- In [11], the AIS-based Fraud Detection Model (AFDM) is introduced as an enhanced fraud detection model in terms of precision and cost which is based on NSA along with Clonal Selection.
  - AFDM utilizes a cloud computing solution for its training phase which leads to certain advantages due to the CC computational features.

The idea upon which this Framework is established is that fraud threats are highly correlated to security challenges without consisting independent problem. The proposed Framework focuses on implementing a set of phases geared towards the entanglement with security issues leading to fraudulent activities.

Fraud Threats Taxonomy

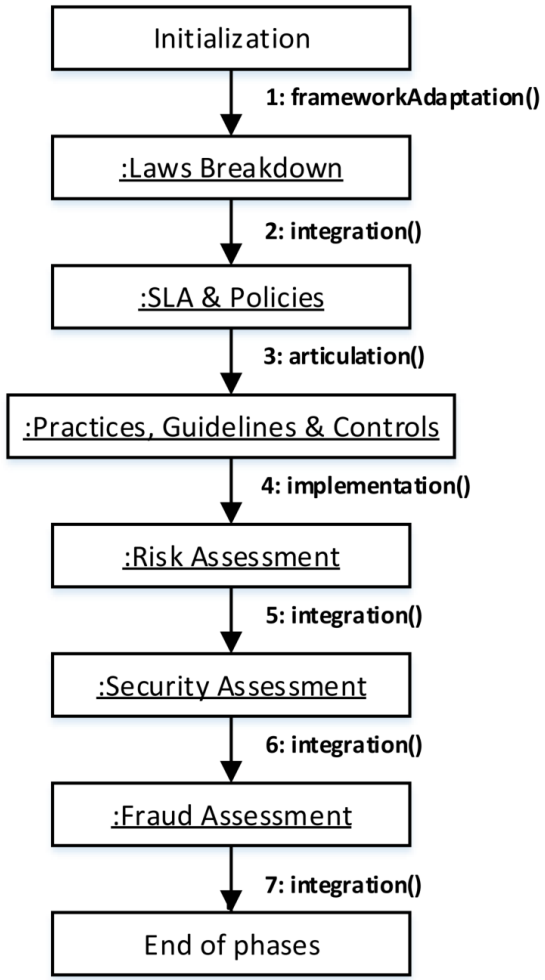
- The cloud attacks (i.e. DDoS, Hijacking, Wrapping) can be leveraged as the initial phase of a penetration which ultimately aims to succeed a fraud activity.
- The fraud threats are classified into the following categories:
  - skimming,
  - pharming,
  - identity theft,
  - botnets and
  - triangulation schemes.
- An attack scenario aiming to succeed fraud:
  - Following the initial stages of any attack, the attackers coordinate their penetration technique with respect to the detected vulnerabilities by the reconnaissance.
  - Then, they exploit the vulnerabilities and gain control over internal services and systems so as to acquire passwords and sensitive information such as the cardholders data in order to initiate fraudulent activities.

Framework Phases

The scope of the Cloud InfoSec Framework is to support the architectural and operational decisions, which form the security and governance controls mitigating fraud threats.

The proposed framework consists of a solution that exploits already developed methods and tactics in order to confront vulnerabilities which lead to fraudulent activities.

The Cloud InfoSec Framework is composed of six distinct phases.



Collaboration diagram of Cloud InfoSec Framework Phases.

Phases Analysis

Laws Breakdown:

- Due to the distributed nature of CC environments, the CSPs are involved in economies of many countries with a significant **positive result**, a great number of potential customers.
- As a result, careful attention must be focused on the challenges that surface by the diversity of laws and regulations that apply in every country in which the CSPs facilities reside.
- By analyzing the national laws in the context of which the CC environment operates and provides the end-services, the CSPs take into account the necessary provisions and implement the imposed constraints with scope to achieve legal compliance.

Phases Analysis

Laws Breakdown:

- In the case that the provided service is a SaaS with focus group any individual in a specific country, then the legislation concerning the processing of personal data is to be acknowledged.
- In the event that the individuals are Community citizens of a Member-State of the European Union (EU), then the legal instructions which have to be implemented should be assigned by:
  - the General Data Protection Directive (GDPR) 2016/679 [15] and
  - the Directive on Security of Networks and Information Systems (NIS Directive) [16].

Phases Analysis

Laws Breakdown:

- In the context of the proposed Framework which aims to fraud threats disclosure, the CSP must comply with the obligations laid down by fraud-related regulations.
- Fraud-related regulations are:
  - the Directive 2009/136/EC [17],
  - the Directive 97/7/EC [18],
  - the Directive 2005/29/EC (Unfair Commercial Practices Directive) [19],
  - the Directive 93/13/EEC [20] on unfair terms in consumer contracts and
  - the Directive 2000/31/EC (E-Commerce Directive) [21].

Phases Analysis

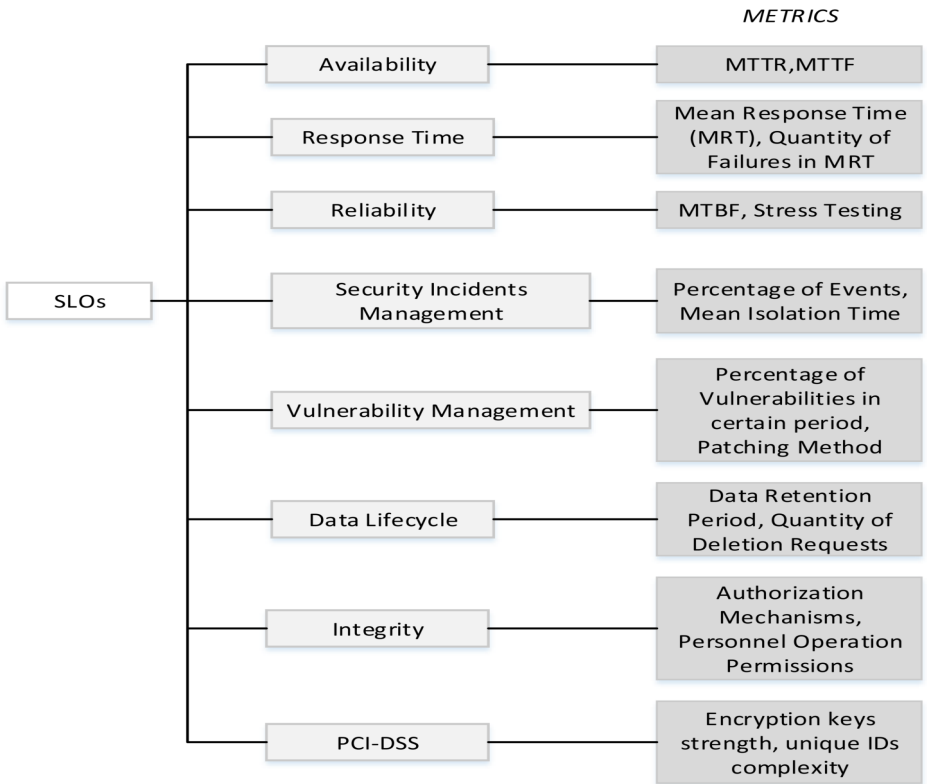
SLA & Policies:

- Through the SLA the CSPs are able to prove that they exhibit compliance to certain operational specifications and standards which are required in order to avoid the negative effects of fraud attacks.
- The role of SLA with regard to fraud, is to:
  - lay a rights and responsibilities section which establishes the duties and rights of both parties, CSP and customers, in order to achieve security transparency.
  - determines the objectives which should be met during the end-services provision and sets the stage for privacy and trust among the agreeing parties through the orchestration of Service Level Objectives (SLOs).

Phases Analysis

SLA & Policies:

- CSPs facilitating access to mission-critical services are expected to deliver in a constant basis, proof that the SLOs enforcement is performed effectively, through SLO metrics.



SLO Metrics.

Phases Analysis

SLA & Policies:

- The policies articulation should be implemented by following specific criterions when the CSP delivers mission-critical services.
- Through the policies, uniformity could be achieved concerning their approach on certain dimensions of CC environment such as the security and privacy measures with regard to fraudulent activities.
- In view of fraud threats mitigation, an *anti-fraud team* should be established and operate by following the policy which determines the fraud risk management operations.

Phases Analysis

Practices, Guidelines & Controls:

- The CSP should develop the appropriate provisions in order to implement the instructions issued by the policies and the employed standards (e.g. PCI-DSS).
- The guidelines articulation will fulfil the needs and objectives set down by the policies and imposed by the legislation.
- The controls are integral component of the CSPs' operation in order to achieve effective risk mitigation.
  - Controls' main objective is to implement the minimum measures so as to accomplish a balanced relation among the level of security and usability that mission-critical services require.

Phases Analysis

Risk Assessment:

- Aiming to accomplish effective risk assessment and address the risks thoroughly, a classification of risks is performed in the following categories:
  - *Organizational and Policy Risks*. The CSPs deviations from their obligations concerning the reporting of the SLOs adequate enforcement consists of a significant risk which can potentially affect the customers' data.
  - *Legislation Risks*. In high-risk countries, the national regulations do not define data protection guidelines as well as the privacy of data and the civil rights of natural people are not applicable [22].
  - *Technical Risks*. Due to the scaling mechanisms which permit fast resource allocation according the demand, the CC environment is susceptible to resource exhaustion, which can be leveraged by Distributed Denial-of-Service (DDoS) attacks.

Phases Analysis

Risk Assessment:

- The risk level indicates the possibility of a fraud attack to succeed and consists of a combination of threats and vulnerabilities.
- In order to manage the described risks, the CC architecture should be divided into two distinct layers of risk namely, the **organizational layer** and the **business mission layer**.
- The definition of risk layers permits association between the attacks and the impact of them against the CC environment.

Phases Analysis

Security Assessment:

- The security assessment identifies PII and system information that can be leaked due to inadequate safeguards.
- This procedure consists of steps such as:
  - active and passive reconnaissance,
  - services' enumeration,
  - networks' mapping,
  - services' exploitation,
  - privileges escalation and
  - trace deletion.
- These steps contribute to the scope of the security assessment which is to define the minimum information the attacker could gain so as to exploit the **cloud boundary**.

Phases Analysis

Security Assessment:

- The cloud boundary is divided into two distinct perieters.
  - *Outside Perimeter*:The Outside Perimeter extends among the computing entities that are visible to the clients.The business mission risk layer belongs to this perimeter. Inside this perimeter also reside limited PII and information about specific CC systems and mechanisms.
  - *Inside Perimeter*: The Inside Perimeter extends among the intranets of the environment. The organizational risk layer belongs to this perimeter. This perimeter hosts PII and critical operational data.
- A wide spectrum of tools and techniques shoud be orchestrated in order to identify the vulnerabilities and the attack vectors.
- The aggregation of the assessments results leads to the vulnerabilities determination that can be leveraged for exploitation.

Phases Analysis

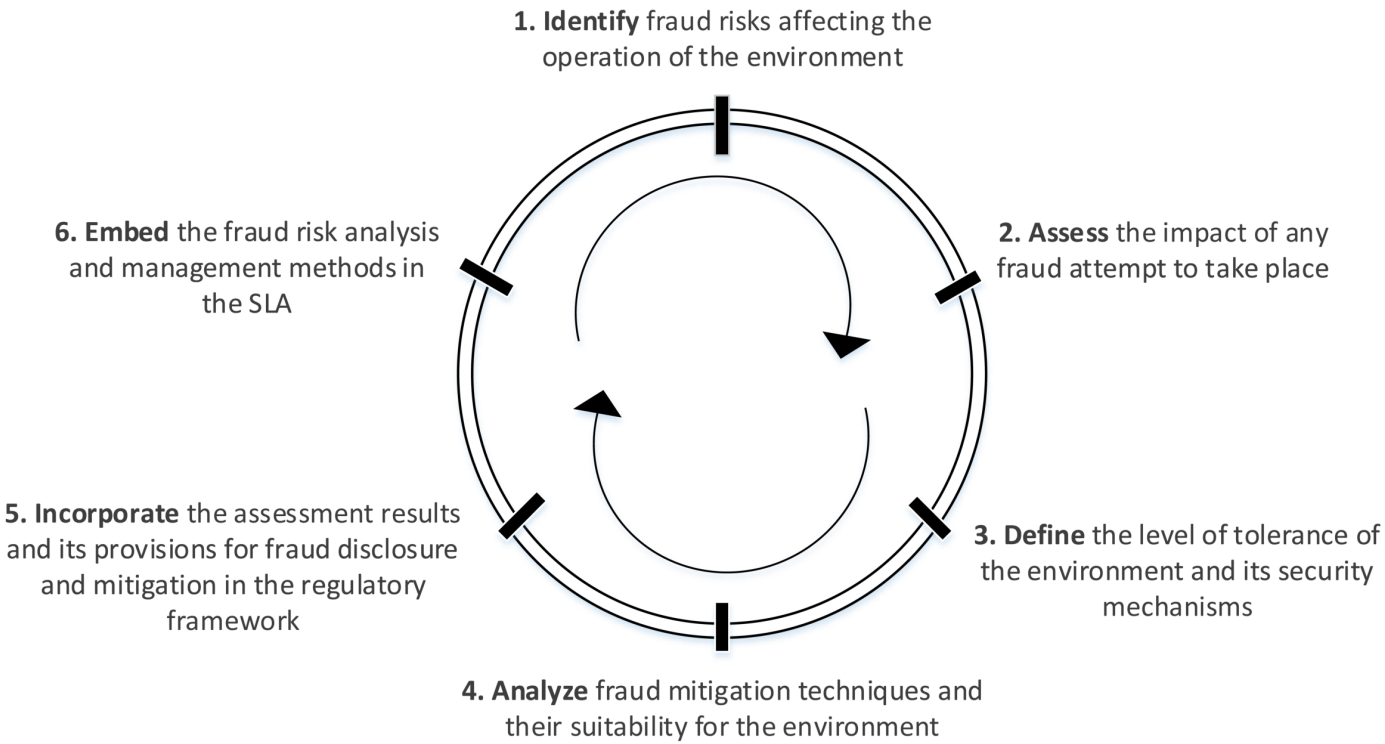
Fraud Assessment:

- The fraud assessment is a procedure performed by the fraud operator in the CC environment, the **anti-fraud team**.
- The implementation of this procedure is initiated by identifying opportunities and vectors to commit fraud both in the *outside* and *inside* perimeter.
- Two main fraud risks for the CC environments are:
  - The **misappropriation of assets** by interacting entities (e.g. clients, personnel) due to the distributed nature of assets. The CSPs threatened assets are all of them which, by the time they are breached have negative impact on the objectives set by the SLA concerning the end-service.
  - The **corruption** is the process of exposure of confidentiality and misuse of cardholder data for private gain by the perpetrator.

Phases Analysis

Fraud Assessment:

- For the purpose of confronting these risks and therefore mitigate the most dangerous fraud threats, the CSP should implement the steps depicted on the **Fraud Assessment Cycle**.



Fraud Assessment Cycle.

Assessment & Gap Analysis

- A cloud scenario is orchestrated in order to evaluate the Cloud InfoSec Framework's effectiveness.
- This scenario consist of many potential attack vectors for fraud perpetrators and bears a close resemblance to reality.
- *Scenario Analysis*: a bank integrates into its business plan a mobile cloud-based service in order to grant access to its clients portfolio so as to enable management of digital credit cards, banking accounts and movements.

Assessment & Gap Analysis

Critical Gaps:

- The integration of fraud detection and prevention mechanisms beyond the measures orchestrated for the organizational layer in context of the second and the third phases.
  - Detection mechanisms and preventive control procedures should be designed and implemented with regard to the end-service without confining its performance.
- The mobile application may behave differently in the case that fraud detection mechanisms perform real-time analysis of data transactions.
- The CC security services, data encryption schemes coupled with fraud detection and prevention mechanisms impact throughput and delay the end-services provision.
  - These delays should be assessed against the nature of mobile applications attributes such as any additional delays due to the coverage of Radio Access Networks (RANs) and the added over-head by the mobile network carrier.

Assessment & Gap Analysis

Critical Gaps:

- Part of the anti-fraud teams' role should be the training of the CSP's personnel following professional standards.
  - The gap lies on the side of the CSPs personnel while the perpetrators exploit their social enginneering skills as an intermediate stage in order to accomplish disclosure of confidential data
- By training the personnel, informing it about the potential threats, it will eventually possess adequate knowledge to support the Frameworks implementation and report malicious activities.
- A gap inheres on the fact that the Framework phases are implemented openly in the CC environment without concealment from the CSPs unauthorized personnel.
  - The Frameworks phases, should remain confidential and the operation of fraud detection and prevention mechanisms should be concealed for the purpose of avoiding **fraud threats** relating to

Conclusions

Synopsis

- Few researchers have addressed the issue of fraudulent activities on cloud.
- The proposed Cloud InfoSec Framework assembles a highly efficient security architecture across the abstraction layers of a CC environment.
- Considerable insight has been gained with regard to the characteristics which should be taken into consideration on the CC paradigm considering mitigation of fraudulent activities.

Conclusions

Future Work!

- The CC defense mechanisms should be enhanced regarding the nefarious usage of CC resources or the abuse of X-as-a-Service (XaaS).
- Work needs to be done on governmental or regional legislation to strengthen the cross-border guidelines with respect to fraud due to the distributed nature of CC environments.
- It is recommended the standardization of a Fraud related Regulatory Framework in European level so as to serve as a basis for CSPs operating on Member-States of the EU.

8th International Conference on Information, Intelligence, Systems and Applications
28, 29 and 30 August 2017, Golden Bay Hotel, Larnaca, Cyprus

Thank you for the attention!
Questions?