Modeling Vulnerabilities and Threats in Cloud Services

Computer Engineering Department

San Jose, California

Professor Weider D. Yu

Maryam Runiassy

Yijun Yin

May 13-15, 2014

Contents

Contents

Introduction

The importance of studying Cloud security

- Cloud Computing is a combination of Networking, Virtualization, Web Application, and other technologies.
- This combination has a lot of potentials to enhance the power of computation world.
- It offers many benefits to its customers:
  - Ubiquitous on-demand access to services on a pay-as-you-go basis.
  - Minimizing the cost of building IT infrastructures and maintenance requirements.

Introduction (Cont.)

- **The importance of studying Cloud security (Cont.)**
  - Despite all these benefits, many businesses are reluctant to accept cloud mainly for having security concerns.
  - Thus, gaining a comprehensive understanding of cloud security is the first and most important step toward building a secure cloud.

Introduction (Cont.)

- **Our goal in this work:**
  - Reviewing currently existing approaches toward understanding cloud security.
  - Introducing a fishbone model to demonstrate the relation between Cloud threats and vulnerabilities.
  - Providing guideline for both Cloud providers and users to enhance the security.

Introduction (Cont.)

- **Existing approaches for studying Cloud security**
  - With the focus on cloud service delivery models (SaaS, PaaS, IaaS) security issues.
  - With the focus on most prevalent security issues and threats in cloud security.
  - With the focus on identifying the security issues that cloud inherits from its building technologies.
  - A combination of all above.

Introduction (Cont.)

- **Existing approaches for studying Cloud security (What is missing?)**
  - A few of those works try to demonstrate the relation between cloud threats and vulnerabilities.
  - Most of these few studies even fail to distinguish threats from vulnerabilities, and thus use these terms interchangeably and cause ambiguity.

Introduction (Cont.)

- **Our approach and contribution**
  - We group Cloud threats into six main categories.
  - We identify the vulnerabilities causing each threat.
  - We build a fishbone model to demonstrate the relationships between Cloud threats and vulnerabilities.
  - We rate each category based on CSA's published papers to identify the most important threats and compare their importance to the others.
  - We briefly introduce guidelines and countermeasure against each threat group.

Contents

Cloud Security Model

- Data loss or leakage
- People
- Web application technologies
- Virtualization
- Cloud service controls and standards
- Communication

Cloud Security Model (Cont.)

An introduction to the security model

- We introduce a fishbone model to show vulnerabilities that cause each cloud threat.
- Our model has six main bones (threat categories): Data loss or leakage, People, Web application technologies, Virtualization, Cloud service controls and standards, and communication.
- Why these 6 bones?
  - In simple words, Cloud combines technologies such as web and virtualizations to deliver on-demand services via network by following certain standards
  - This brief definition roughly introduces the six main categories that we introduce in this model.

Cloud Security Model (Cont.)

- **An introduction to the security model (Cont.)**
  - Some subcategories overlap or are related.
  - We tried to place each threat under the most relevant category based on the fact that if the flaws, which cause this threat, are directly related to that specific category.
  - Ex. DOS attacks are both related to web application and services, people, or virtualization, yet what allows people or a malicious virtual machine to launch DoS attacks are existing flaws in web and application technologies.

Cloud Security Model (Cont.)

- **An introduction to the security model (Cont.)**
  - Vulnerability refers to existing flaws in a system.
  - Threat refers to an agent that exploits existing vulnerabilities in a system.
  - Vulnerability Vs. Threat: vulnerabilities are exposing a system to be compromised, while threats are actors that try to take advantage of vulnerabilities.

Cloud Security Model (Cont.)

- **Data loss or leakage**
  - Unauthorized access to data
    - Weak or obsolete or none cryptography methods.
    - Poor key management procedures.
  - Malicious manipulation and failure of data import or export
    - Data backup plan.
    - Cloud providers subcontract the backup service to third-party organizations.

Cloud Security Model (Cont.)

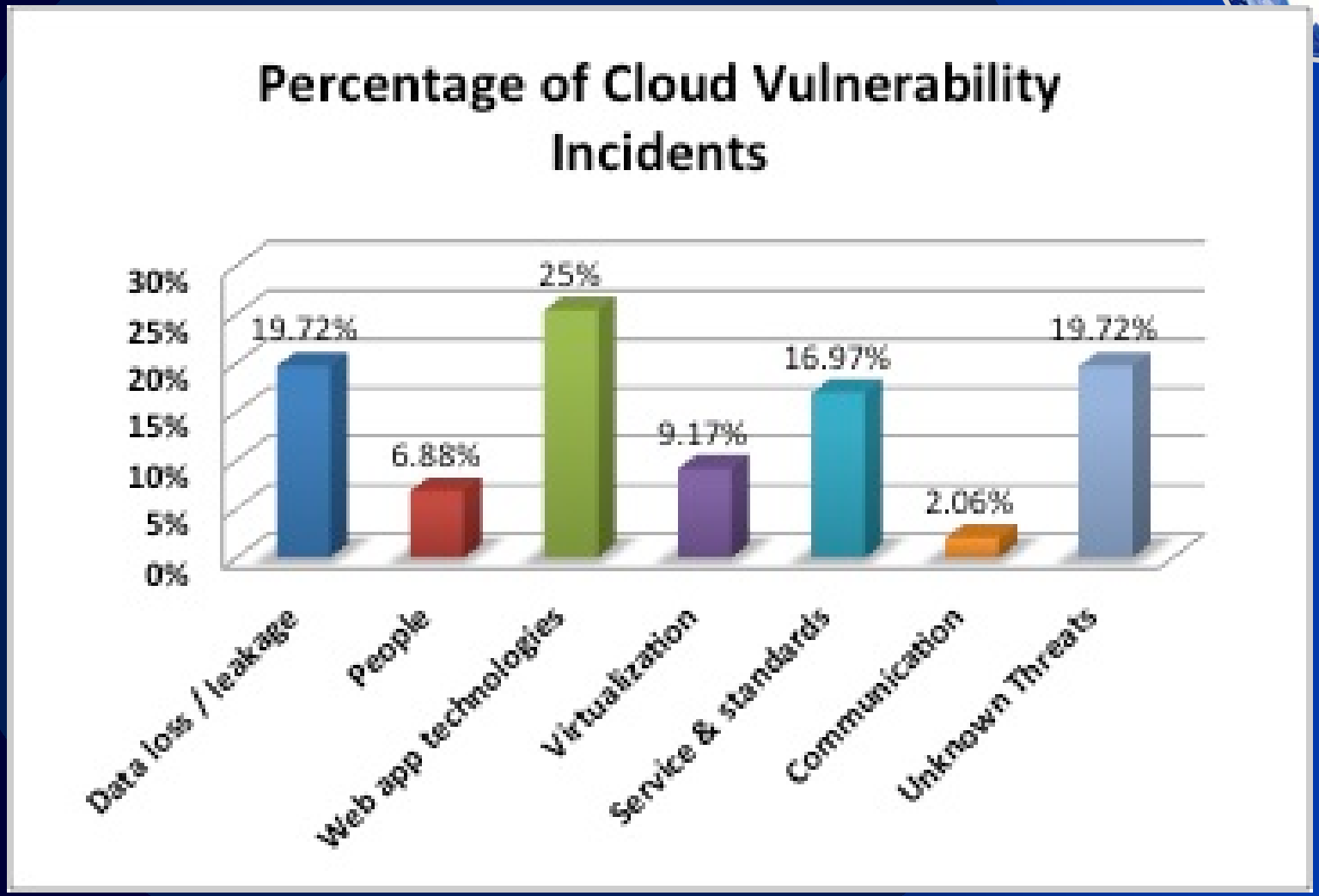
- **Data loss or leakage (Cont.)**
  - Failing to segregate shared data
    - The data belonging to various users is resided at the same location.
  - Incomplete data deletion
    - The resources de-allocated from one user will be assigned to another user later.
    - The deleted data can be recovered as long as the physical disk destruction does not be carried out.

Top Threats Rating

The data we used

- Provided by Cloud Security Alliance (CSA).
- “Top Threats to Cloud Computing” from 11,491 news articles.
- Cloud-computing-related outages from 39 news sources.
- Between Jan 2008 and Feb 2012.
- The total number of Cloud vulnerability incidents is 172.

Top Threats Rating Result



Contents

Suggestions and Guidelines

- **Data Loss or Leakage**
  - Use latest and powerful cryptography to encrypt data.
  - Specify data destruction strategies in SLA.
  - Apply digital signatures

Suggestions and Guidelines (Cont.)

People

- Clarify the administrative control policies.
- Follow a strict hiring policy that ensures the identity and background of their employees, especially the administrators.
- Train their users and inform them about secure and insecure behaviors that might put the system at risk.
- Apply controls on data input forms and consider exceptional cases of user interaction with systems and predict strong enough countermeasures.

Suggestions and Guidelines (Cont.)

Web Application Technologies

- Use SSL to protect session id.
- API keys should be used by Web and Cloud services to identify third-party applications using the services.
- Apply controls over raw user input.
- Limit the permissions of the Web application when accessing the database.
- Defend against the packet flood itself.
- Limit the resources allocated to each user using quotas or handle one request per user at a time by synchronizing on the user's session.

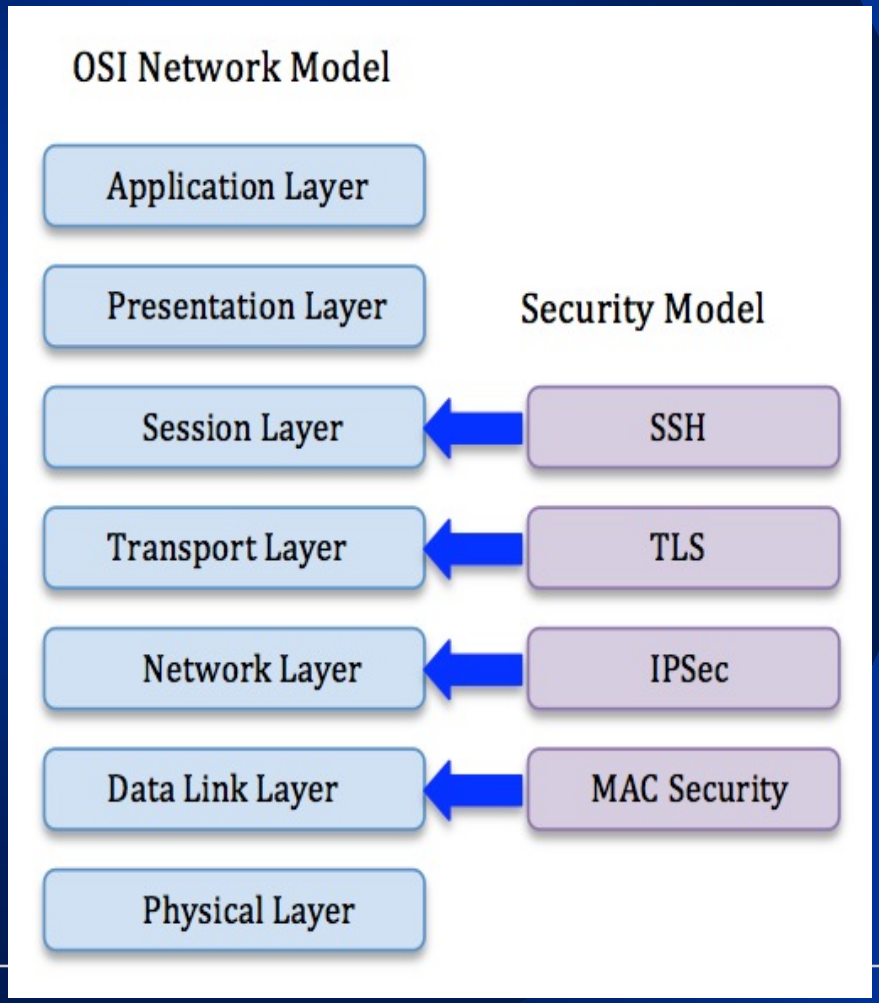
Suggestions and Guidelines (Cont.)

Cloud Service Controls and Standards

- Fully understand the services satisfying the business requirements.
- Discuss the requirements to see if the CSP covers the needs in terms of service quality and provided security.
- Make a plan for migrating to another Cloud environment that completely covers all their requirements to avoid vendor lock-in.

Suggestions and Guidelines (Cont.)

- **Communication**



Contents

Conclusion

- We proposes a new approach in studying Cloud Computing threats, vulnerabilities and their relations.
  - We categorized Cloud main threats into six groups and identified the vulnerabilities that cause each threat.
  - Then, we used a fishbone model to demonstrate the existing connections between Cloud threats and vulnerabilities.
  - We also offered guidelines that both CSPs and Cloud customers can follow to avoid these threats and build more secure Cloud environments.
  - Finally, we ranked each category of threats to identify the most critical ones based on reports published by CSA.
- Our next step would be searching real word use-cases to support our approach in designing the suggested fishbone model.

San José State
UNIVERSITY

Thank You !