

Security and Privacy in Cloud Computing

Ragib Hasan
Johns Hopkins University
en.600.412 Spring 2010

Lecture 2
02/01/2010

Threats, vulnerabilities, and enemies

Goal

Learn the cloud computing threat model by examining the assets, vulnerabilities, entry points, and actors in a cloud

Technique

Apply different threat modeling schemes

Assignment for next class

- Review: Thomas Ristenpart et al., **Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds**, proc. ACM CCS 2009.

- Format:
  - Summary: A brief overview of the paper, 1 paragraph (5 / 6 sentences)
  - Pros: 3 or more issues
  - Cons: 3 or more issues
  - Possible improvements: Any possible suggestions to improve the work

- Due: 2.59 pm 2/8/2010
- Submission: By email to rhasan7@jhu.edu (text only, no attachments please)

Threat Model

A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions

Steps:

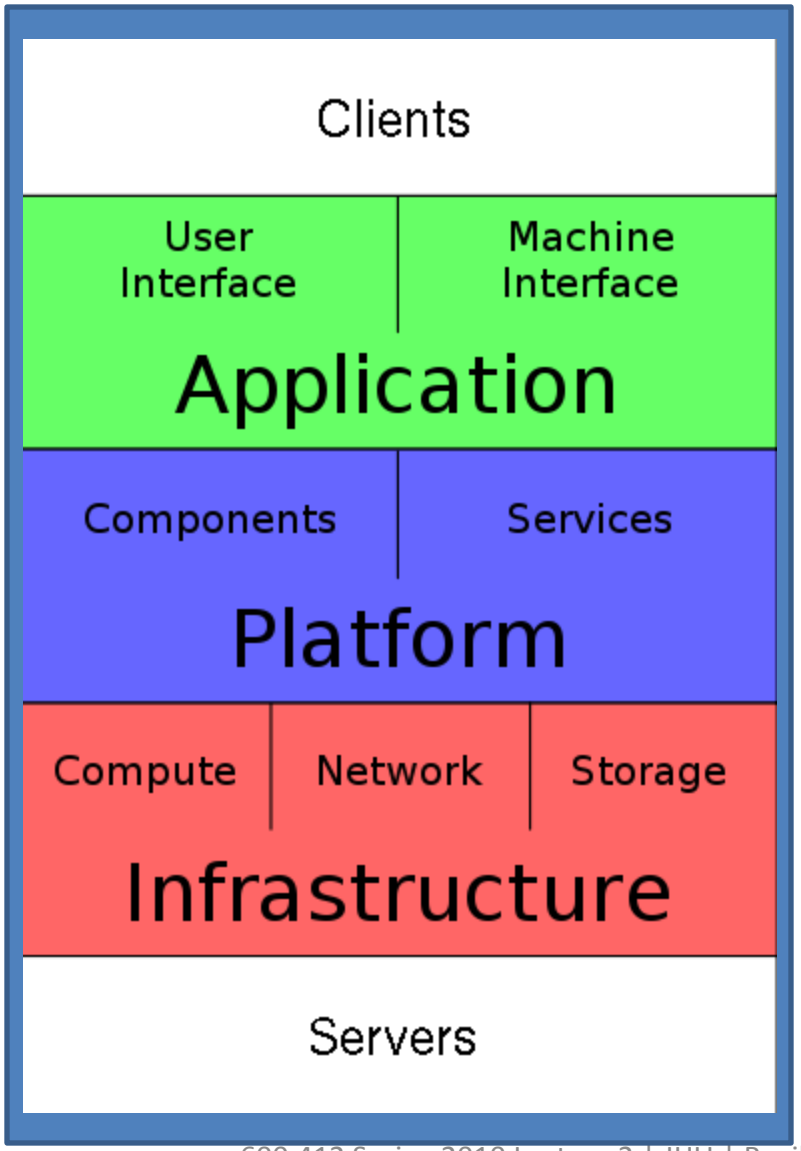
- Identify attackers, assets, threats and other components
- Rank the threats
- Choose mitigation strategies
- Build solutions based on the strategies

Threat Model

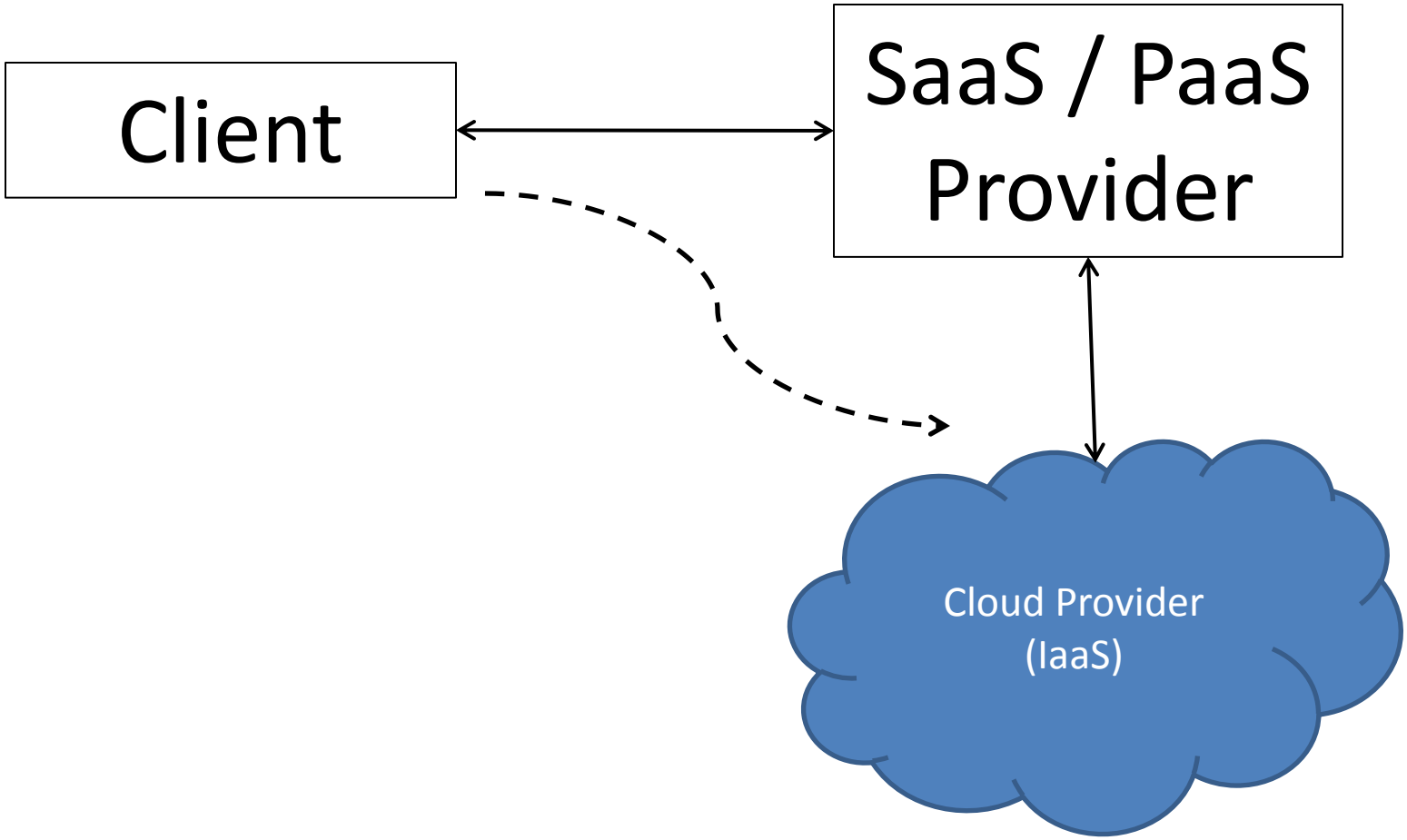
Basic components

- Attacker modeling
  - Choose what attacker to consider
  - Attacker motivation and capabilities
- Assets / Attacker Goals
- Vulnerabilities / threats

Recall: Cloud Computing Stack



Recall: Cloud Architecture



Attackers

Who is the attacker?

Insider?

- Malicious employees at client
- Malicious employees at Cloud provider
- Cloud provider itself

Outsider?

- Intruders
- Network attackers?

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication

Attacker Capability: Cloud Provider

- What?
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns

Attacker motivation: Cloud Provider

- Why?
  - Gain information about client data
  - Gain information on client behavior
  - Sell the information or use itself
- Why not?
  - Cheaper to be honest?
- Why? (again)
  - Third party clouds?

Attacker Capability: Outside attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS

Attacker goals: Outside attackers

- Intrusion
- Network analysis
- Man in the middle
- Cartography

Assets

Assets (Attacker goals)

- Confidentiality:
  - Data stored in the cloud
  - Configuration of VMs running on the cloud
  - Identity of the cloud users
  - Location of the VMs running client code

Assets (Attacker goals)

- Integrity
  - Data stored in the cloud
  - Computations performed on the cloud

Assets (Attacker goals)

- Availability
  - Cloud infrastructure
  - SaaS / PaaS

Threats

Organizing the threats using STRIDE

- **S**poofing identity
- **T**ampering with data
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privilege

Typical threats

Threat type	Mitigation technique
Spoofing identity	•Authentication •Protect secrets •Do not store secrets
Tampering with data	•Authorization •Hashes •Message authentication codes •Digital signatures •Tamper-resistant protocols
Repudiation	•Digital signatures •Timestamps •Audit trails

[STRIDE]

Typical threats (contd.)

Threat type	Mitigation technique
Information disclosure	•Authorization •Privacy-enhanced protocols •Encryption •Protect secrets •Do not store secrets
Denial of service	•Authentication •Authorization •Filtering •Throttling •Quality of service
Elevation of privilege	•Run with least privilege

[STRIDE]

Summary

- A threat model helps in designing appropriate defenses against particular attackers

- Your solution and security countermeasures will depend on the particular threat model you want to address

Further Reading

Frank Swiderski and Window Snyder , “Threat Modeling “, Microsoft Press, 2004

The STRIDE Threat Model