고려대학교
KOREA UNIVERSITY

KU-The Future

Cloud computing – Chapter 6

Heonchang Yu

Distributed and Cloud Computing Lab.

Basic Terms and Concepts

- Confidentiality
  - characteristic of something being made accessible only to authorized parties

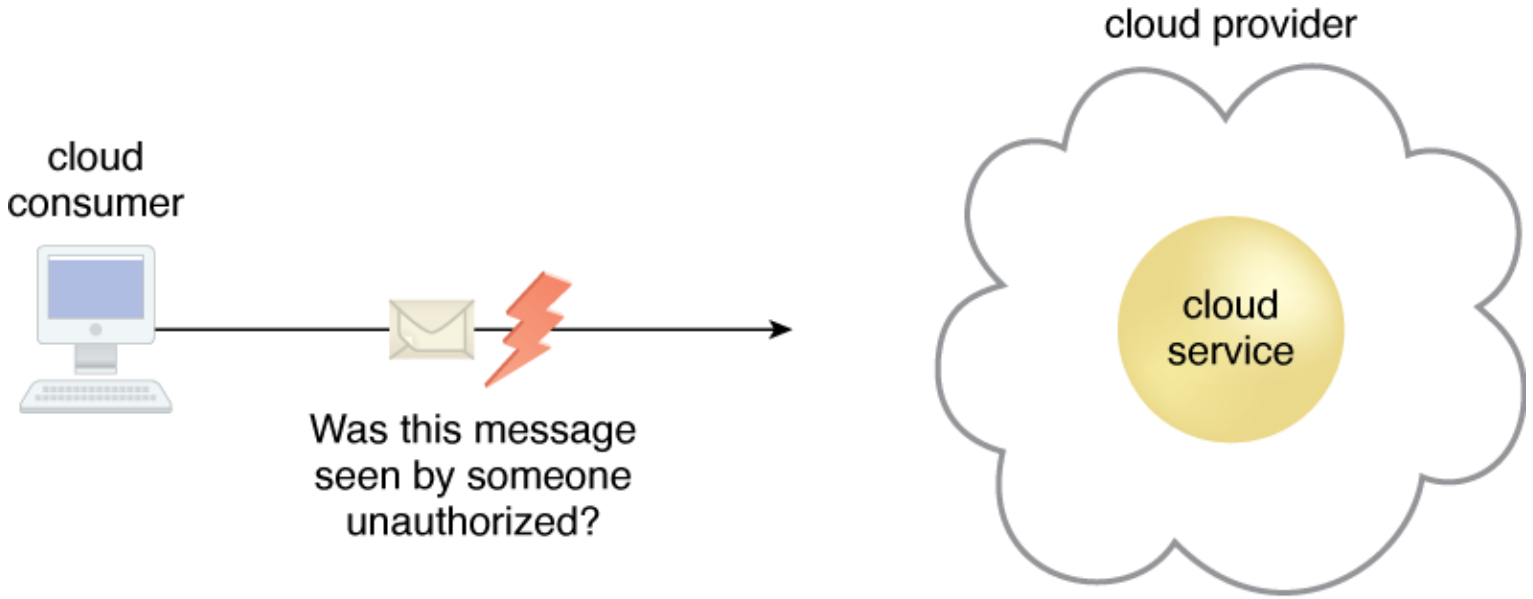

Figure 6.1. The message issued by the cloud consumer to the cloud service is considered confidential only if it is not accessed or read by an unauthorized party

Basic Terms and Concepts

- Integrity
  - Characteristic of not having been altered by an unauthorized party

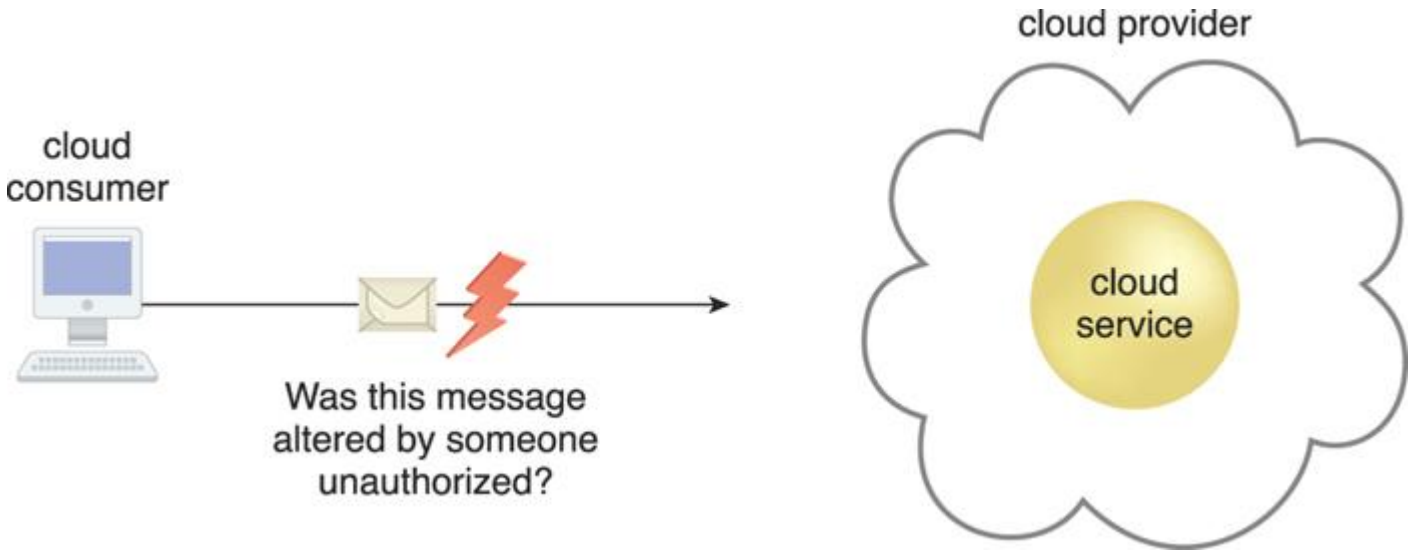

Figure 6.2 The message issued by the cloud consumer to the cloud service is considered to have integrity if it has not been altered.

Basic Terms and Concepts

- Authenticity
  - characteristic of something having been provided by an authorized source
  - non-repudiation, which is the inability of a party to deny or challenge the authentication of an interaction
- Availability
  - characteristic of being accessible and usable during a specified time period
  - availability of cloud services : a responsibility that is shared by the cloud provider and the cloud carrier

Basic Terms and Concepts

- Threat
  - Potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm
  - Designed to exploit known weaknesses, referred to as vulnerabilities
  - results in an *attack*
- Vulnerability
  - Weakness that can be exploited either because it is protected by insufficient security controls, or because existing security controls are overcome by an attack

Basic Terms and Concepts

- Risk
  - Possibility of loss or harm arising from performing an activity. Two metrics that can be used to determine risk:
    - ✓ Probability of a threat occurring to exploit vulnerabilities in the IT resource
    - ✓ Expectation of loss upon the IT resource being compromised
- Security Controls
  - Countermeasure used to prevent or respond to security threats and to reduce or avoid attack
- Security Policies
  - A set of security rules and regulations

Threat Agents

- Threat Agents
  - Entity that poses a threat because it is capable of carrying out an attack
  - Cloud security threat can originate either internally or externally, from humans or software programs.

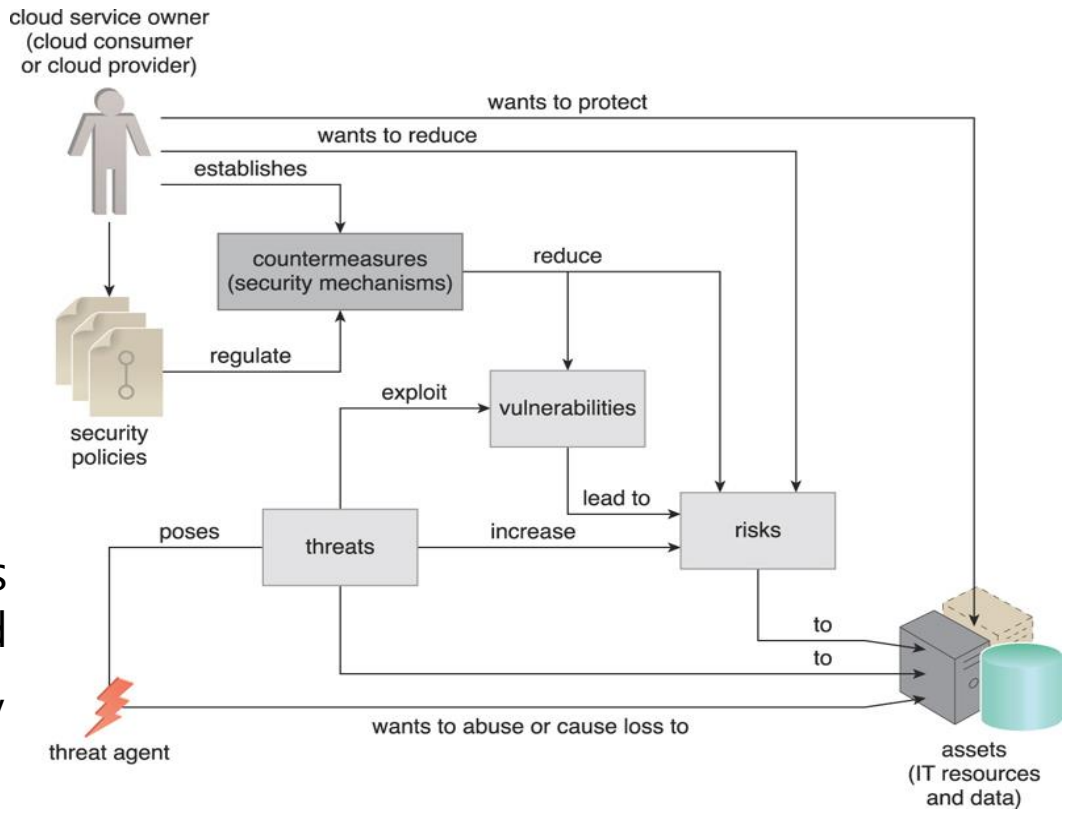

Figure 6.3. How security policies and security mechanisms are used to counter threats, vulnerabilities, and risks caused by threat agents

Threat Agents

- Anonymous Attacker
  - Non-trusted cloud service consumer without permissions in the cloud
  - Anonymous Attackers often resort to committing acts like bypassing user accounts or stealing credentials.

Figure 6.4. The notation used for an anonymous attacker

Threat Agents

- Malicious Service Agent
  - Can intercept and forward the network traffic that flows within a cloud
  - Typically exists as a service agent
  - Exists as an external program able to remotely intercept and potentially corrupt message contents

Figure 6.5. The notation used for a malicious service agent

Threat Agents

- Trusted Attacker
  - Shares IT resources in the same cloud environments as the consumer and attempts to exploit legitimate credentials to target cloud providers and the cloud tenants with whom they share IT resources
  - Unlike anonymous attackers, launch their attacks from within a cloud's trust boundaries by abusing legitimate credentials or via the appropriation of sensitive and confidential information
  - Can exploit including, or launch attacks like DoS
    - Hacking of weak authentication
    - Breaking of encryption
    - Spamming of e-mail accounts

Figure 6.6. The notation that is used for a trusted attacker

Threat Agents

- Malicious Insider
  - Human threat agents acting on behalf of or in relation to the cloud provider
  - Typically current or former employees or third parties with access to the cloud provider's premises
  - Carries tremendous damage potential

Figure 6.7. The notation used for an attack originating from a workstation. The human symbol is optional.

Cloud Security Threats

- Traffic Eavesdropping
  - occurs when data being transferred to or within a cloud is passively intercepted by a malicious service agent for illegitimate information gathering purposes
  - Like packet-sniff attack
  - Because of the passive nature of the attack, it can more easily go undetected for extended periods of time.

Cloud Security Threats

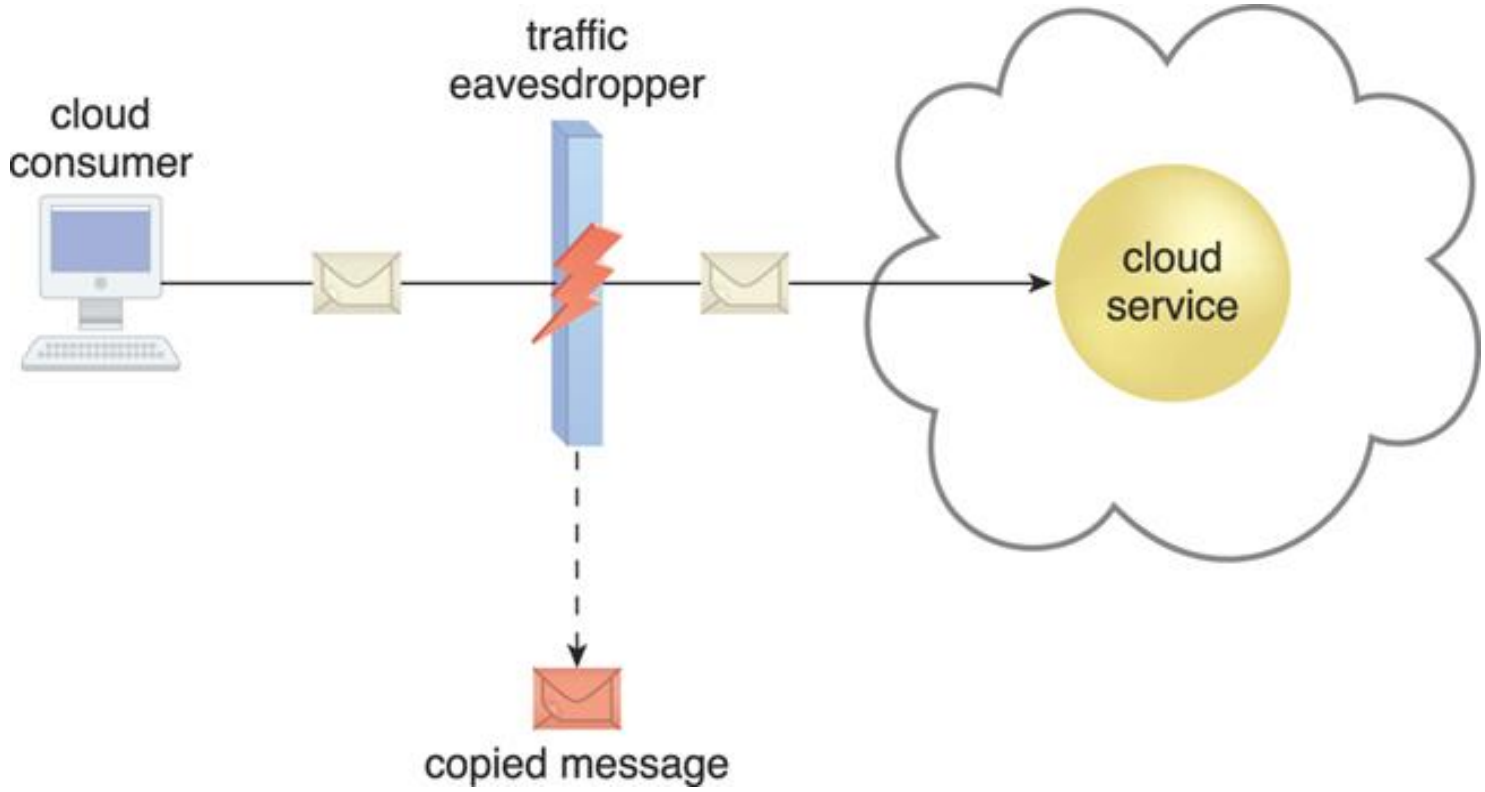

Figure 6.8. An externally positioned malicious service agent carries out a traffic eavesdropping attack by intercepting a message sent by the cloud service consumer to the cloud service. The service agent makes an unauthorized copy of the message before it is sent along its original path to the cloud service

Cloud Security Threats

- Malicious Intermediary
  - Arises when messages are intercepted and altered by a malicious service agent
  - It may insert harmful data into the message before forwarding it to its destination

Cloud Security Threats

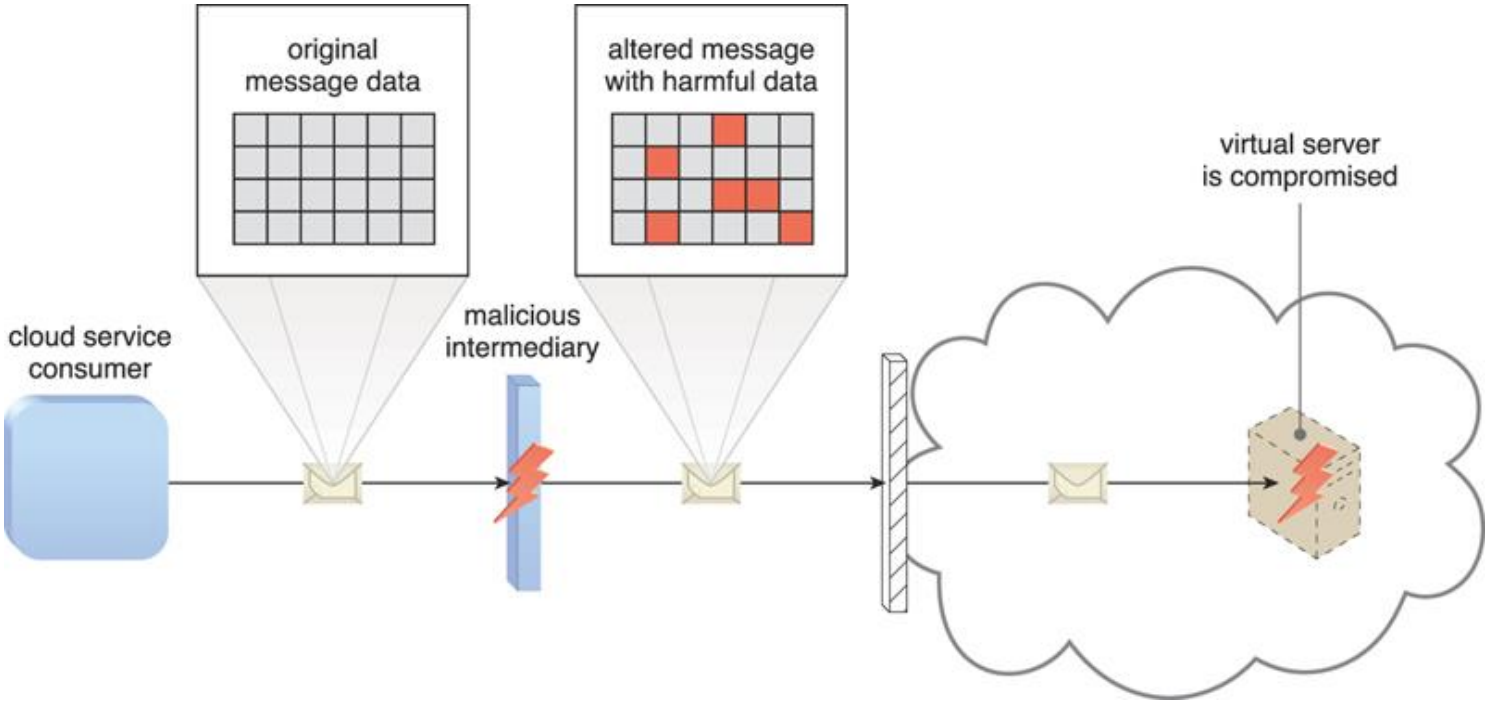

Figure 6.9. The malicious service agent intercepts and modifies a message sent by a cloud service consumer to a cloud service (not shown) being hosted on a virtual server. Because harmful data is packaged into the message, the virtual server is compromised

Cloud Security Threats

- Denial of Service(DoS)
  - Is to overload IT resources to the point where they cannot function properly
    - The workload on cloud services is artificially increased with imitation messages or repeated communication requests.
    - The network is overloaded with traffic to reduce its responsiveness and cripple its performance.
    - Multiple cloud service requests are sent, each of which is designed to consume excessive memory and processing resources.

Cloud Security Threats

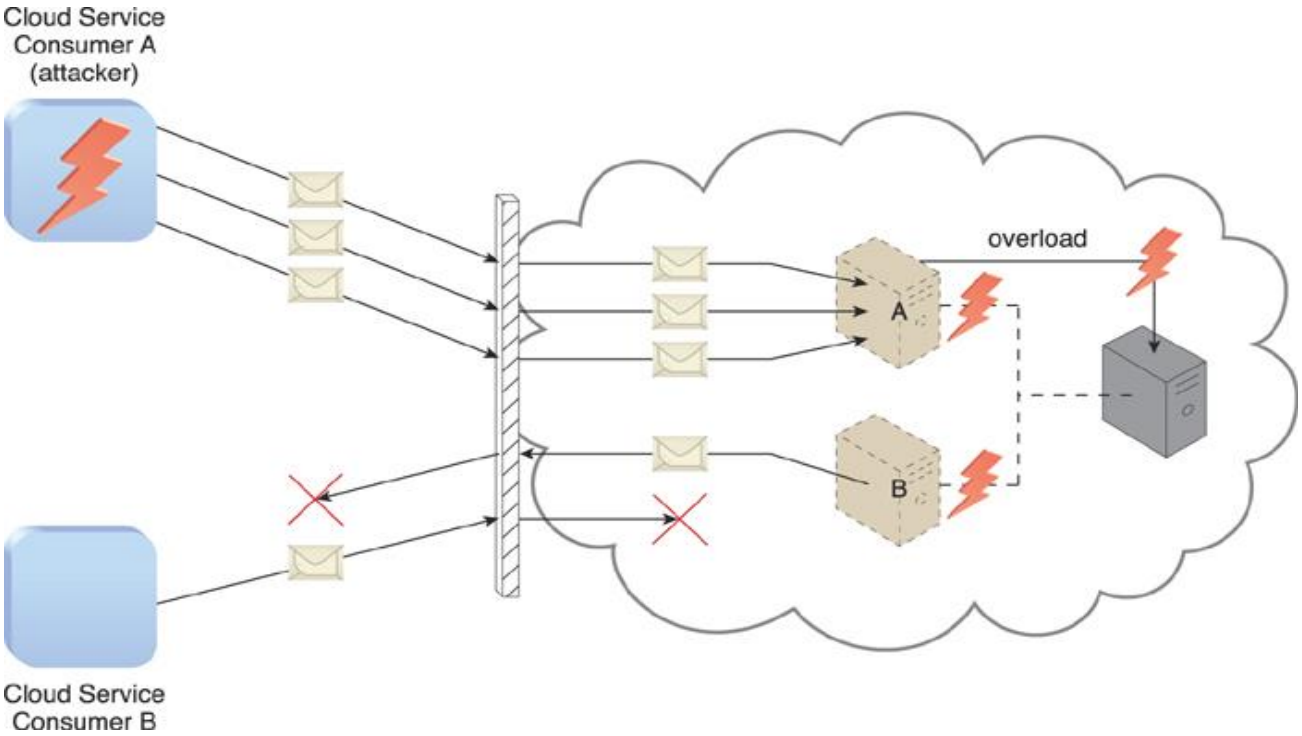

Figure 6.10. Cloud Service Consumer A sends multiple messages to a cloud service (not shown) hosted on Virtual Server A. This overloads the capacity of the underlying physical server, which causes outages with Virtual Servers A and B. As a result, legitimate cloud service consumers, such as Cloud Service Consumer B, become unable to communicate with any cloud services hosted on Virtual Servers A and B

Cloud Security Threats

- Insufficient Authorization
  - Occurs when access is granted to an attacker erroneously or too broadly, resulting in the attacker getting access to IT resources that are normally protected

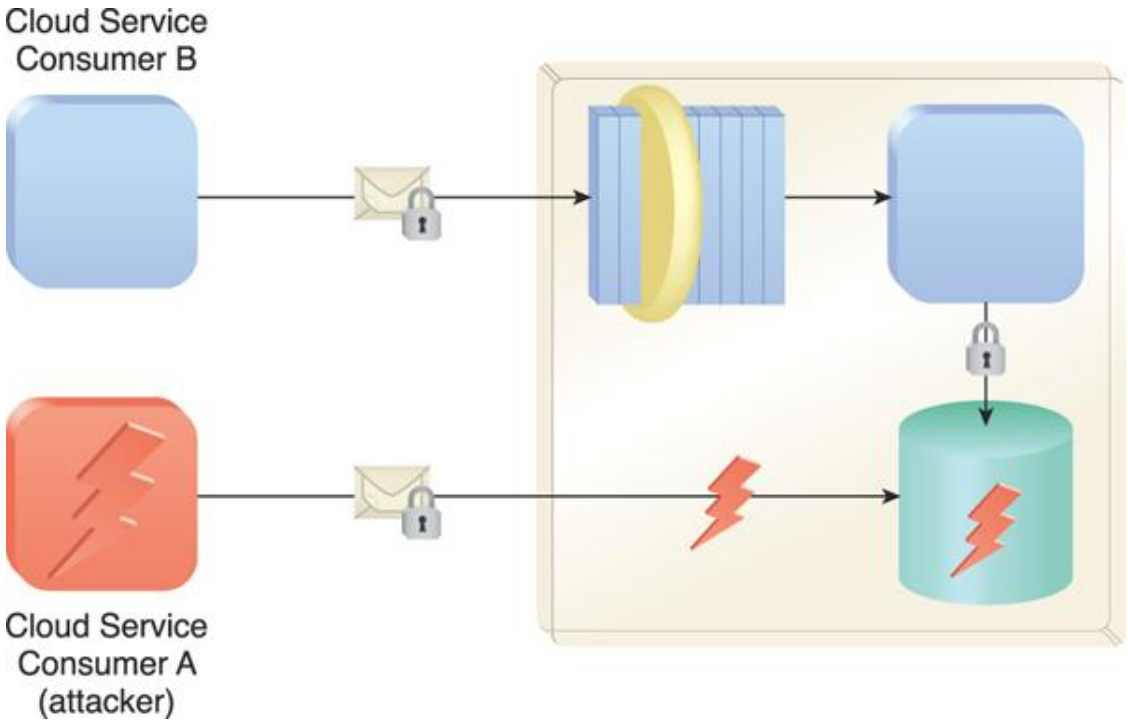

Figure 6.11. Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B)

Cloud Security Threats

– Variation of this attack
  - Weak authentication
  - When weak passwords or shared accounts are used to protect IT resources

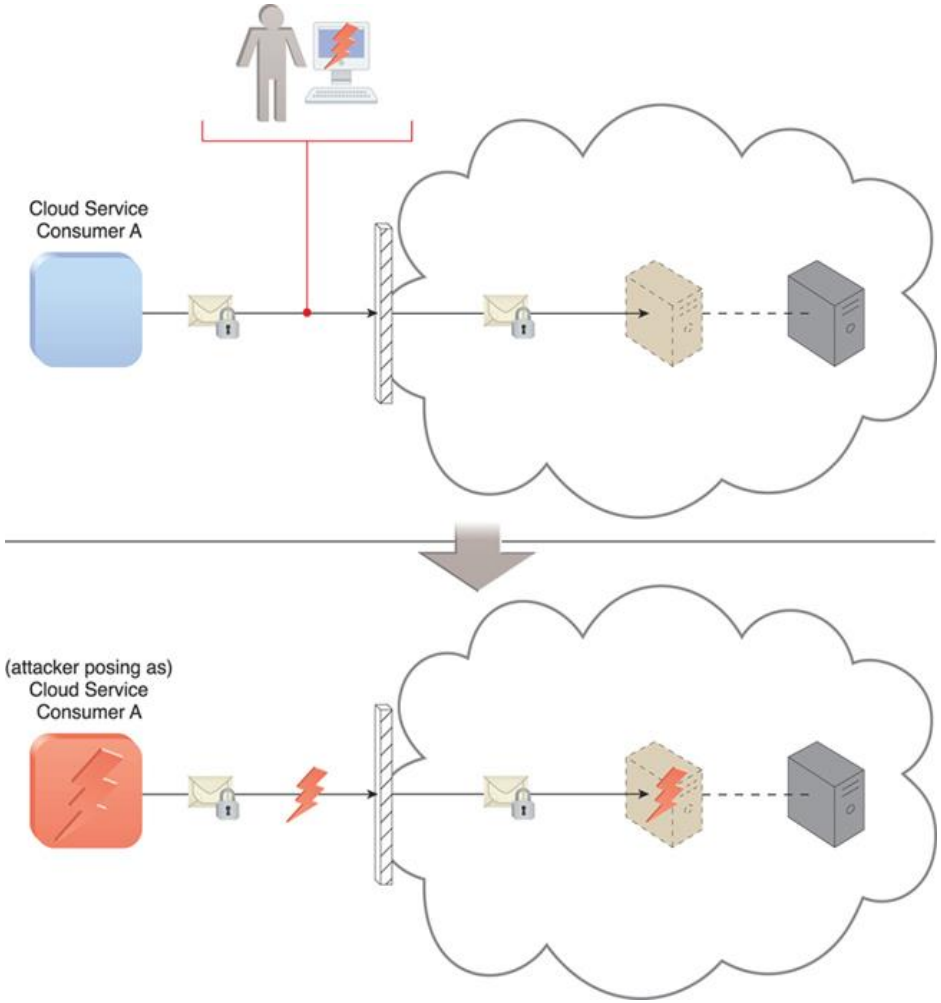

Figure 6.12. An attacker has cracked a weak password used by Cloud Service Consumer A. As a result, a malicious cloud service consumer (owned by the attacker) is designed to pose as Cloud Service Consumer A in order to gain access to the cloud-based virtual server

Cloud Security Threats

- Virtualization Attack
  - Exploits vulnerabilities in the virtualization platform to jeopardize

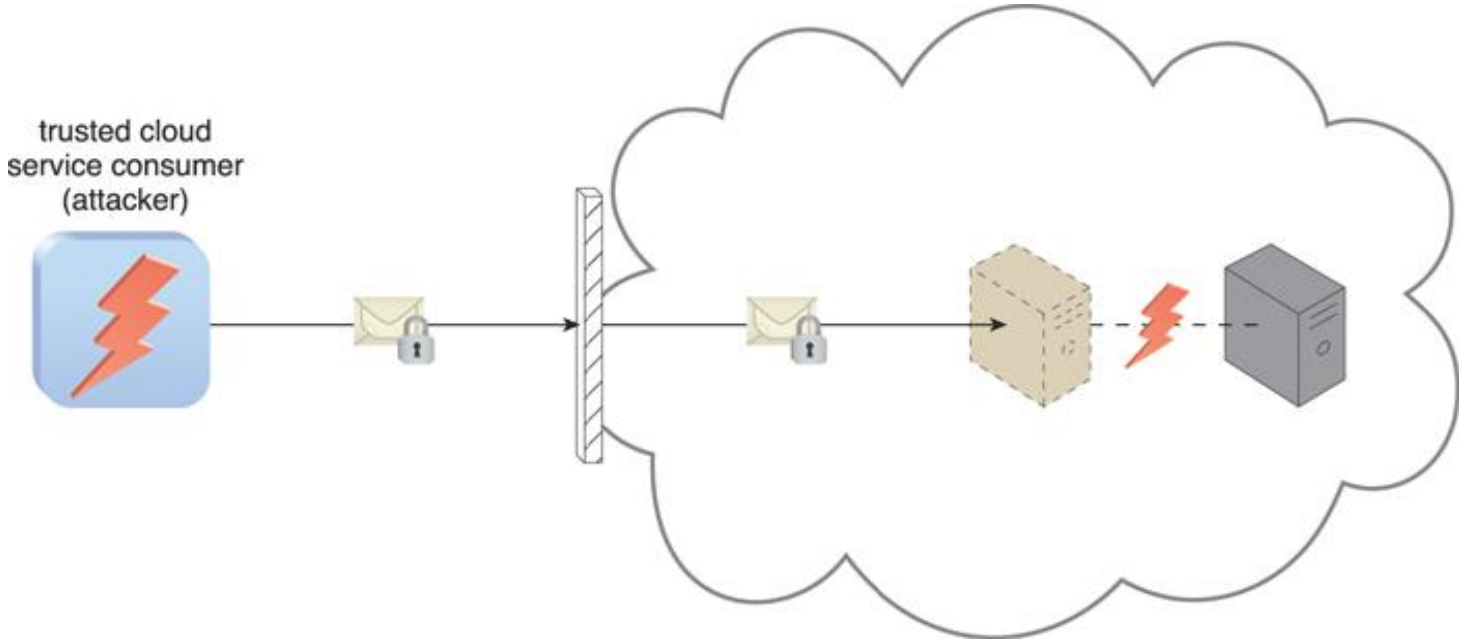

Figure 6.13. An authorized cloud service consumer carries out a virtualization attack by abusing its administrative access to a virtual server to exploit the underlying hardware

Cloud Security Threats

- Overlapping Trust Boundaries
  - If physical IT resources within a cloud are shared by different cloud service consumers, these cloud service consumers have overlapping trust boundaries.
- Malicious cloud service consumers can target shared IT resources with the intention of compromising cloud consumers.

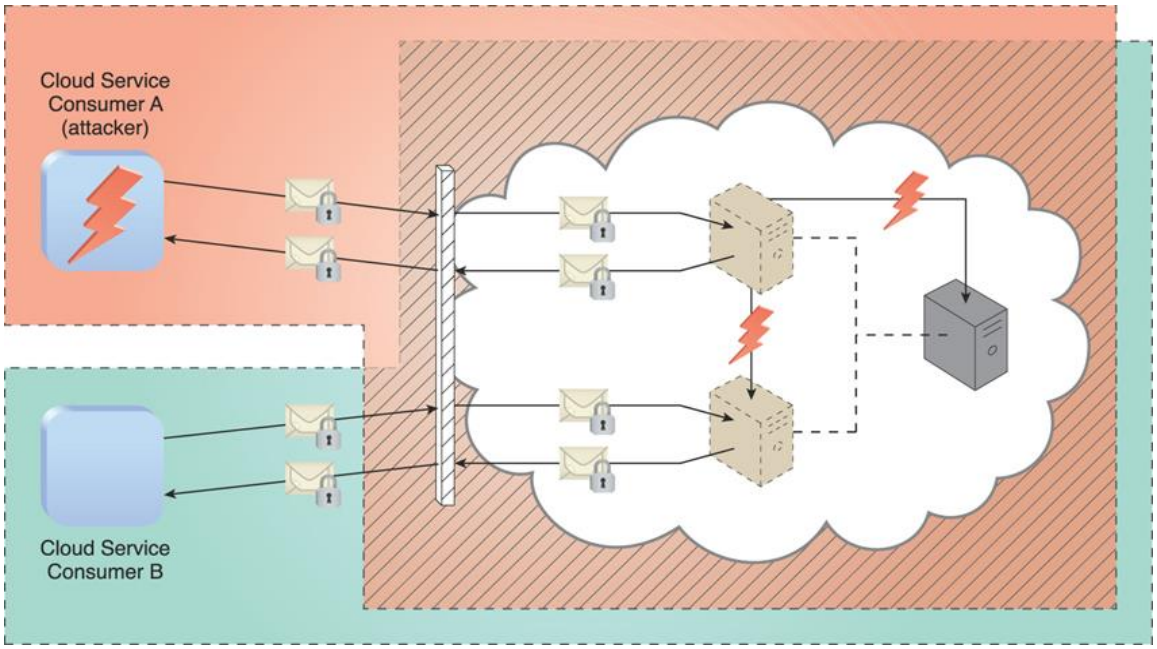

Figure 6.14. Cloud Service Consumer A is trusted by the cloud and therefore gains access to a virtual server, which it then attacks with the intention of attacking the underlying physical server and the virtual server used by Cloud Service Consumer B

Additional Considerations

- Flawed Implementations
  - Substandard design, implementation, or configuration of cloud service deployments can have undesirable consequences, beyond runtime exceptions and failures.
  - Attackers can exploit these vulnerabilities

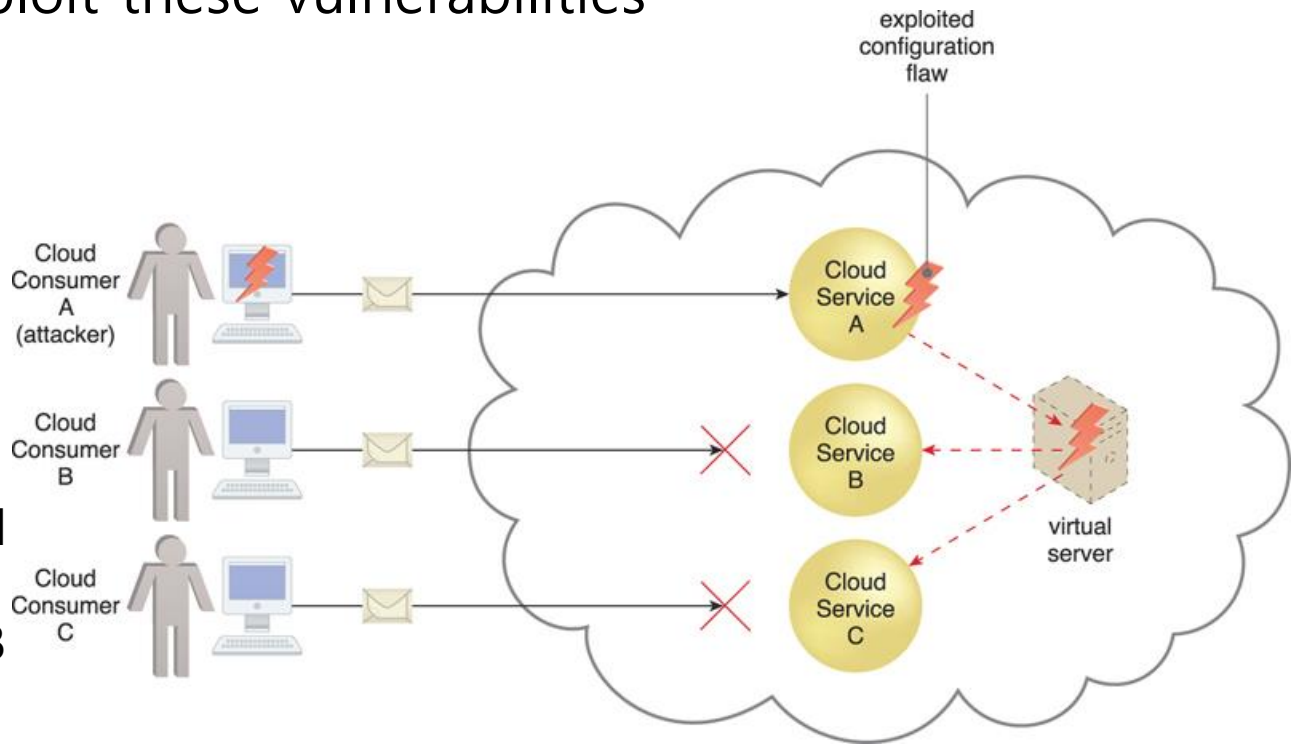

Figure 6.15. Cloud Service Consumer A's message triggers a configuration flaw in Cloud Service A, which in turn causes the virtual server that is also hosting Cloud Services B and C to crash

Additional Considerations

- Security Policy Disparity
  - When a cloud consumer places IT resources with a public cloud provider, it may need to accept that its traditional information security approach may not be identical or even similar to that of the cloud provider.

- Contracts
  - Cloud consumers need to carefully examine contracts and SLAs put forth by cloud providers to ensure that security policies and other relevant guarantees are satisfactory.
  - The greater the assumed liability by the cloud provider, the lower the risk to the cloud consumer.

Additional Considerations

- Risk Management
  - Risk Assessment
    - The cloud environment is analyzed to identify potential vulnerabilities and shortcomings that threats can exploit.
    - The identified risks are quantified and qualified according to the probability of occurrence and the degree of impact in relation to how the cloud consumer plans to utilize cloud-based IT resources.
  - Risk Treatment
    - Mitigation policies and plans are designed during the risk treatment stage with the intent of successfully treating the risks that were discovered during risk assessment.
    - Some risks can be eliminated, others can be mitigated.

Additional Considerations

- Risk Management
  - Risk Control
    - Related to risk monitoring
    - Three-step process to manage
      1. Surveying related events
      2. Reviewing these events to determine the effectiveness of previous assessments and treatments
      3. Identifying any policy adjustment needs

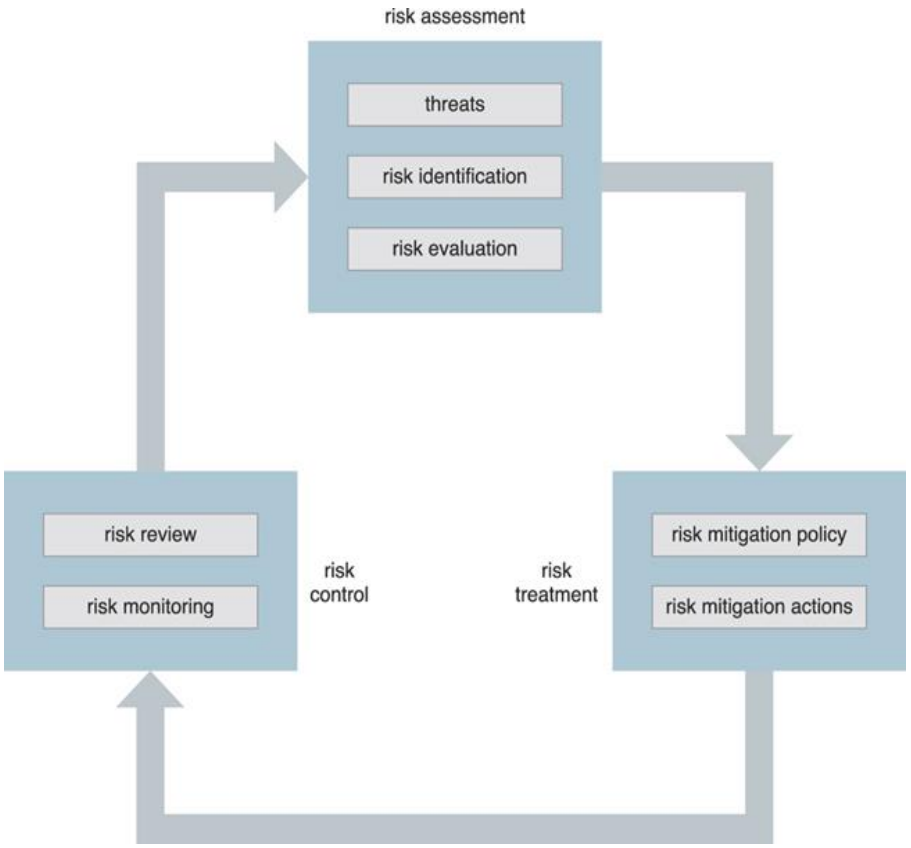

Figure 6.16. The on-going risk management process, which can be initiated from any of the three stages