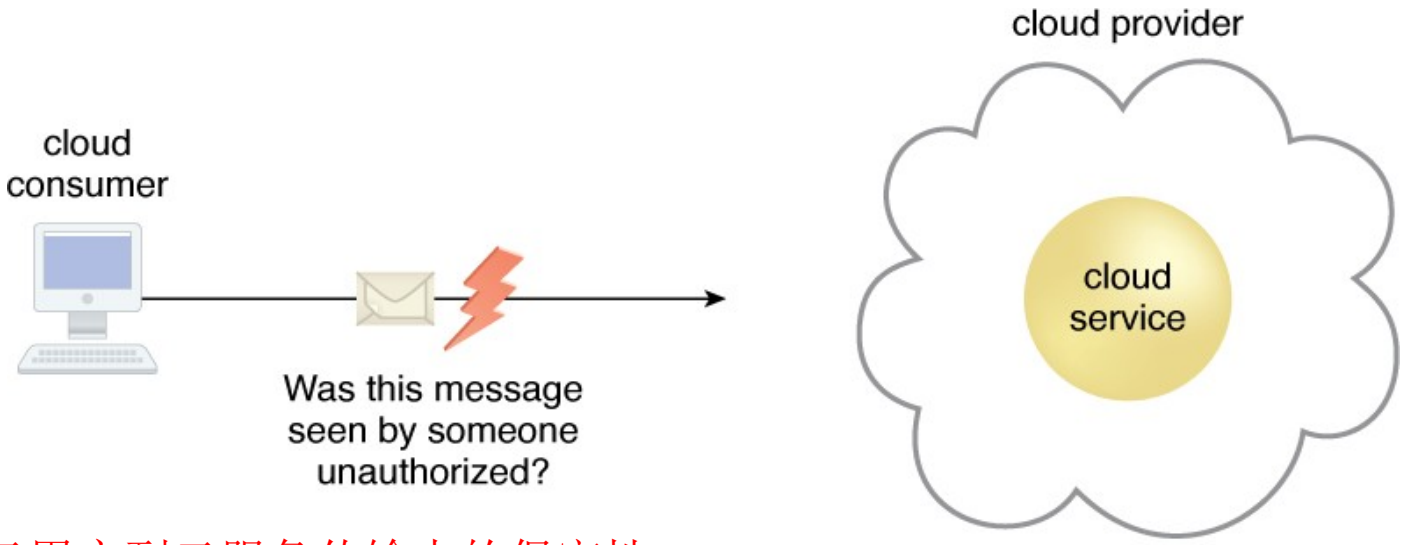
第6章 基本云安全

§6.1 基本术语和概念
§6.2 威胁作用者
§6.3 云安全威胁
§6.4 其他考量

保密性

- 保密性(Confidentiality)是指只有被授权方才能访问的特性
- 在云环境中，保密性主要是关于对传输和存储的数据进行访问限制的。



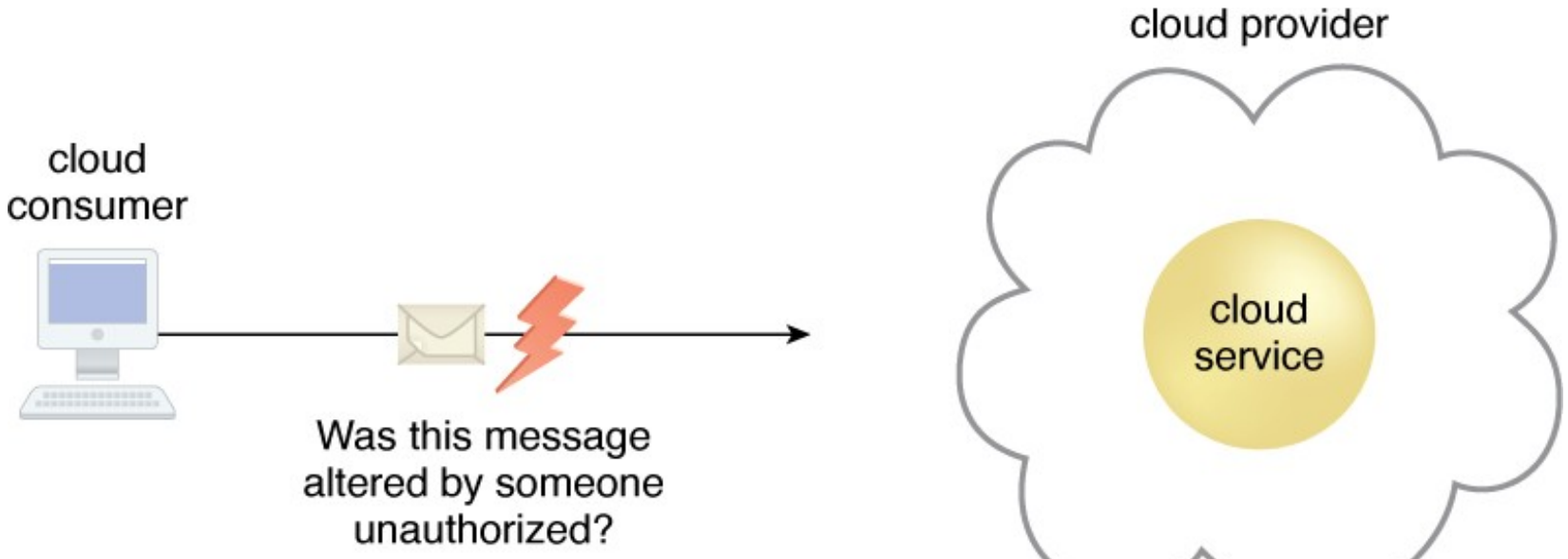
云用户到云服务传输中的保密性

云服务到云用户传输中的保密性？

云端存储的保密性？

完整性

- 完整性(integrity)是指未被未授权方篡改的特性。
  - 具体来说，关系到云中数据完整性的一个重要问题是能否向云用户保证传送到云服务的数据与云服务接收到的数据完全一致，以及从云服务发出与云用户接收到的数据完全一致。



云用户到云服务的完整性

云服务到云用户传输中的完整性？

真实性与可用性

- 真实性(authenticity)是指事务是由经过授权的源提供的这一特性
  - 不可否认的交互中的真实性提供了一种证明，证明这些交互是否是唯一连接到一个经过授权的源的。

- 可用性(availability)是在特定的时间段内可以访问和可以使用的特性

威胁、漏洞和风险

- 威胁(threat)是潜在的安全性违反，可能试图破坏隐私并导致危险。
- 漏洞(vulnerability)是可能是因为安全控制保护不够或者是因为攻击，击败了现有的安全控制而被利用的一种弱点。
- 风险(risk)是指执行一个行为带来损失或危害的可能性。
  - 有两个标准可以用来确定IT资源的风险：

    1、威胁利用IT资源中漏洞的概率

    2、如果IT资源被损害，预期会造成的损失

安全控制、安全机制与安全策略

- 安全控制(Security Controls)是用来预防或响应安全威胁以及降低或者避免风险的对策。

- 安全机制(Security mechanisms)是构成保护IT资源、信息和服务的防御框架的组成部分。---稍后讲安全机制细节

- 安全策略(Security policy)建立了一套安全规则和规章

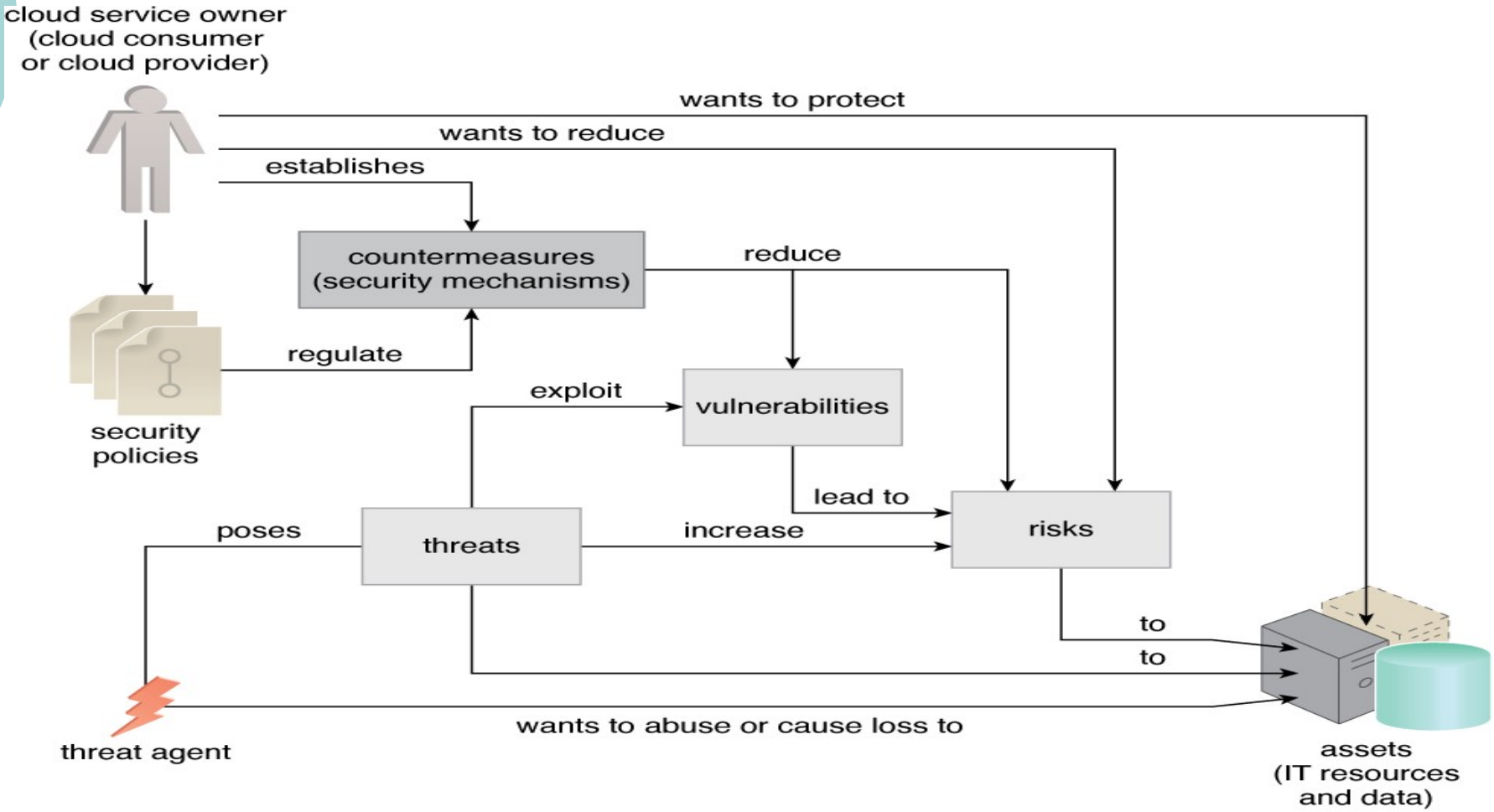
关键点小结

- 保密性、完整性、真实性和可用性是可以与衡量安全性相关联的特性。
- 威胁、漏洞和风险是与衡量和评估不安全性或者安全性缺乏相关联的。
- 安全控制、机制和策略是与建立支持改进安全性的对策和保护措施相关联的。

威胁作用者

- 威胁作用者(threat agent)是引发威胁的实体，因为它能够实施攻击。
- 一个威胁作用者可能来自外部、来自于人、也可能来自于软件程序。
- 在接下来说到的几种不同的攻击者之中，被信任的攻击者和恶意内部者的攻击是威胁最大的。

威胁作用者与对应策略示意图



匿名攻击者

- 匿名攻击者(Anonymous Attacker)是云中没有权限的、不被信任的云服务用户。通常从云边界外部进行攻击。

Figure 6.4 - The notation used for an anonymous attacker.

恶意服务作用者

- 恶意服务作用者(Malicious Service Agent)能截取并转发云内的网络流量，从而恶意地使用或篡改数据。

Figure 6.5 – The notation used for a malicious service agent.

授信的攻击者

- 授信的攻击者(Trusted Attacker)与同一云环境中的云用户共享IT资源，试图利用合法的证书来把云提供者以及他们共享IT资源的云租户作为攻击目标

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

恶意的内部人员

- 恶意的内部人员(Malicious Insider)是人为的威胁作用者，他们的行为代表云提供者或者与之有关，即试图滥用对云资源范围的访问特权的人。

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

关键点小结

- 匿名攻击者是不被信任的威胁作用者，通常试图从云边界外部进行攻击。
- 恶意服务作用者截取网络通信，试图恶意地使用或篡改数据。
- 授信的攻击者是经过授权的云服务用户，具有合法的证书，他们会使用这些证书来访问基于云的IT资源。
- 恶意的内部人员是试图滥用对云资源范围的访问特权的人。

流量窃听

- 流量窃听(Traffic Eavesdropping)是指当数据在传输到云中或在云内部传输时被恶意的服务作用者被动地截获，用于非法的信息收集的目的。
- 这种攻击的目的就是直接破坏数据的保密性，可能也破坏了云用户和云提供者之间关系的保密性。
- 由于这种攻击被动的本质，这种攻击很容易被长时间忽略。

流量窃听

Definition

Traffic eavesdropping occurs when data being transferred to or within a cloud (usually from the cloud consumer to the cloud provider) is passively intercepted by a malicious service agent for illegitimate information gathering purposes.

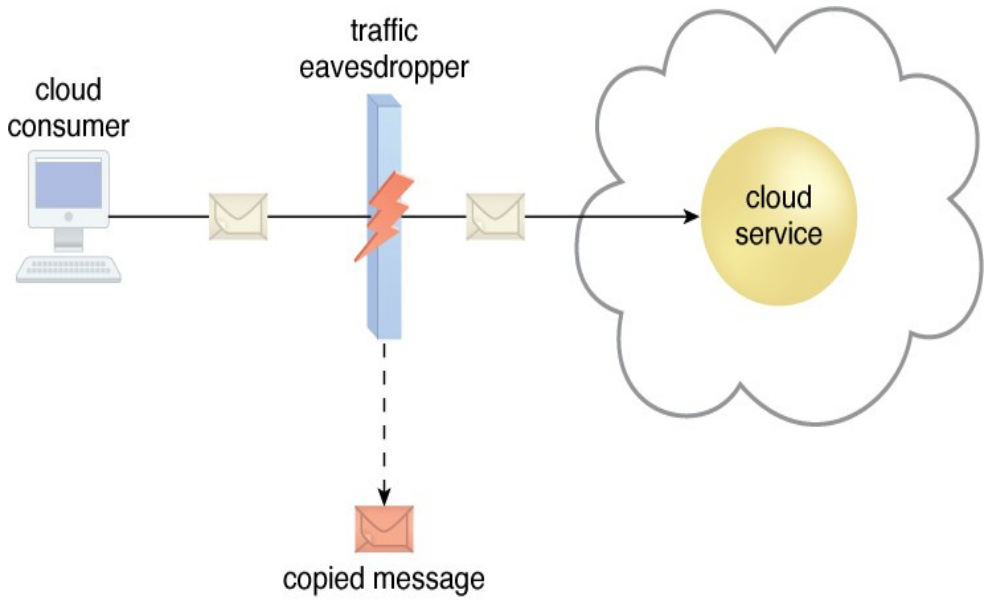


Figure 6.8 – An externally positioned malicious service agent carries out a traffic eavesdropping attack by intercepting a message sent by the cloud service consumer to the cloud service. The service agent makes an unauthorized copy of the message before it is sent along its original path to the cloud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

恶意媒介

- 恶意媒介(Malicious Intermediary)威胁是指消息被恶意服务作用者截获并且被篡改，因此可能会破坏消息的保密性和完整性。
- 它还可能在把消息转发到目的地之前注入有害的数据。
- 一个恶意云用户程序可能带来恶意媒介攻击。

恶意媒介

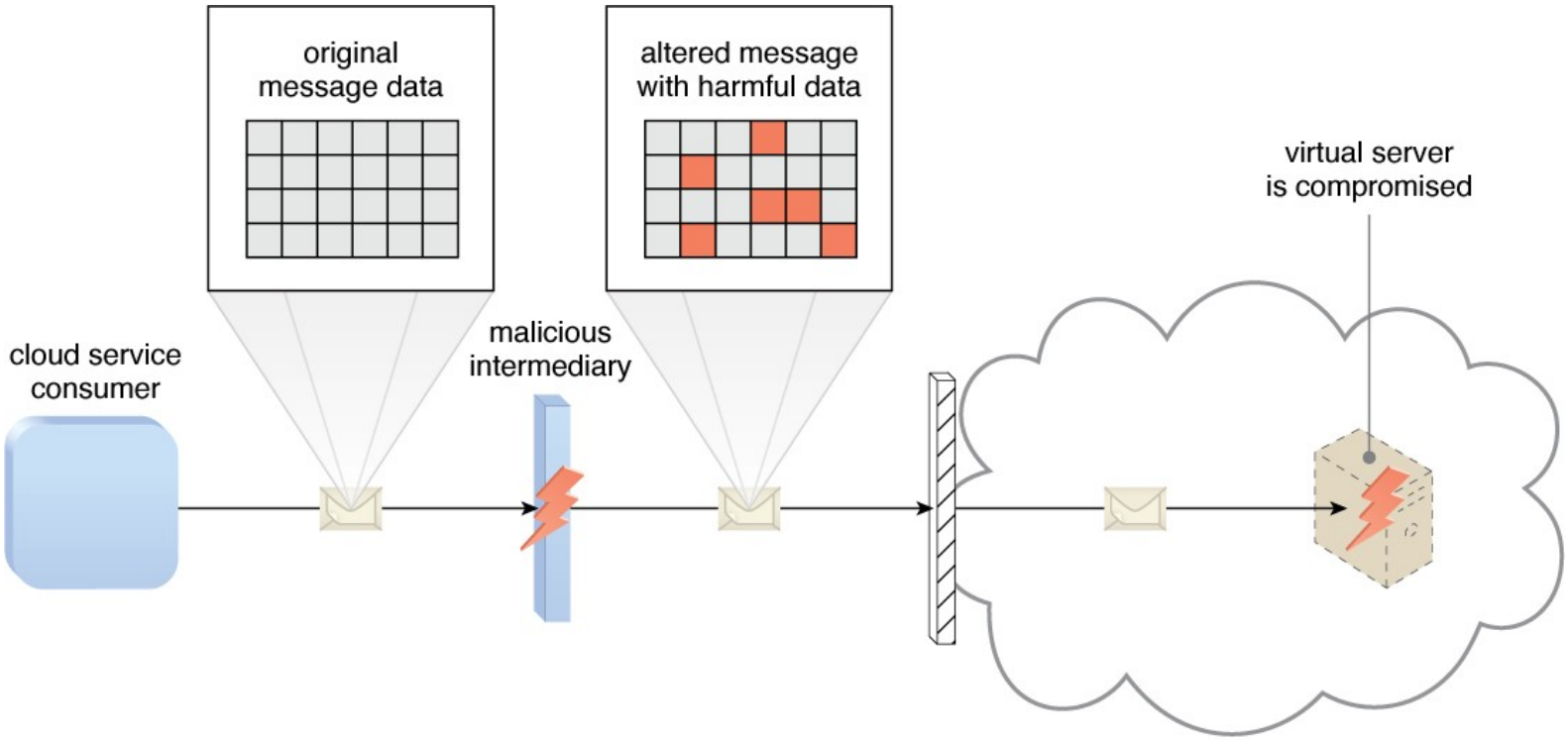


Figure 6.9 – The malicious service agent intercepts and modifies a message sent by a cloud service consumer to a cloud service (not shown) being hosted on a virtual server. Because harmful data is packaged into the message, the virtual server is compromised.

拒绝服务

- 拒绝服务(Denial of Service)攻击的目标是使IT资源过载至无法正确运行。
- 通常是以下方式之一发起的：
  - 云服务上的负载由于伪造的消息或重复的通信请求不正常地增加。
  - 网络流量过载，降低了响应性，性能下降。
  - 发出多个云服务请求，每个请求都设计成消耗过量的内存和处理资源。
- 成功的DoS攻击使得服务器性能恶化或失效。

拒绝服务

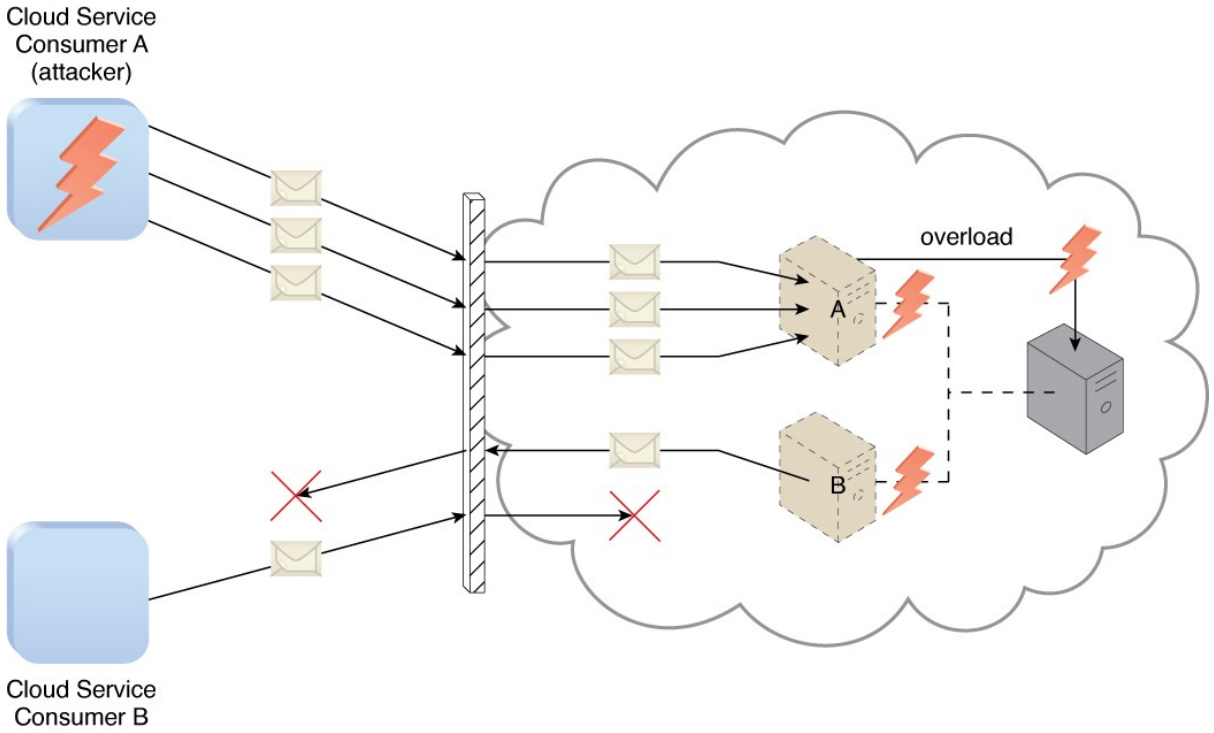


Figure 6.10 – Cloud Service Consumer A sends multiple messages to a cloud service (not shown) hosted on Virtual Server A. This overloads the capacity of the underlying physical server, which causes outages with Virtual Servers A and B. As a result, legitimate cloud service consumers, such as Cloud Service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

授权不足

- 授权不足(Insufficient Authorization)攻击是指错误地授予了攻击者访问权限或是授权太宽泛，导致攻击者能够访问到本应该受保护的IT资源。
- 授权不足的结果通常是攻击者获得了对默写IT资源的直接访问的权利，这些IT资源实现的时候是假设只能是授信的用户程序才能访问的。

授权不足

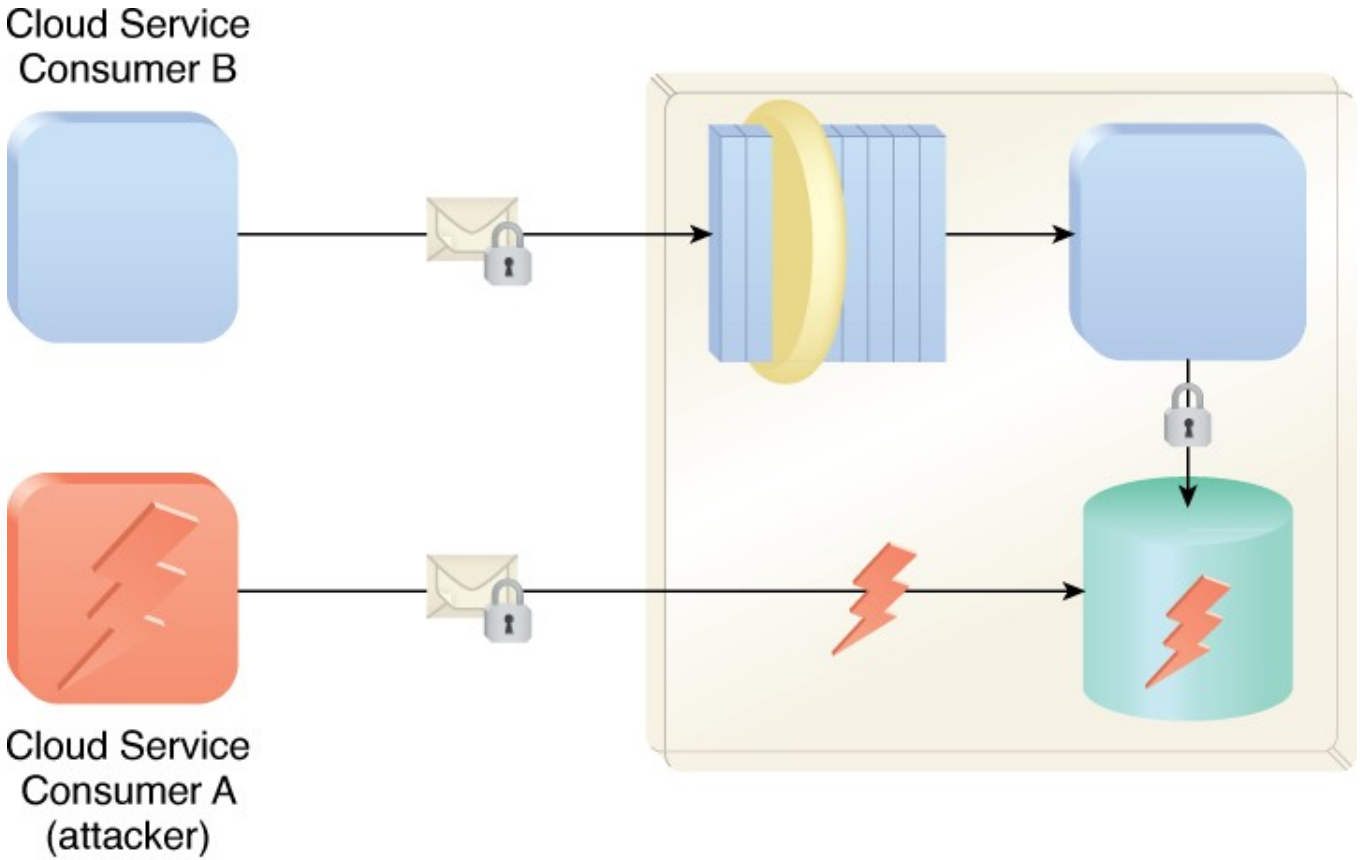


Figure 6.11 – Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B).

虚拟化攻击

两种：

- 虚拟化攻击(Virtualization Attack)利用的是虚拟化平台中的漏洞来危害虚拟化平台的保密性、完整性和可用性。

- 因为云提供者给予云用户对虚拟化的IT资源的管理权限，随之而来的风险就是云用户会滥用这种访问权限来攻击底层物理IT资源。

虚拟化攻击

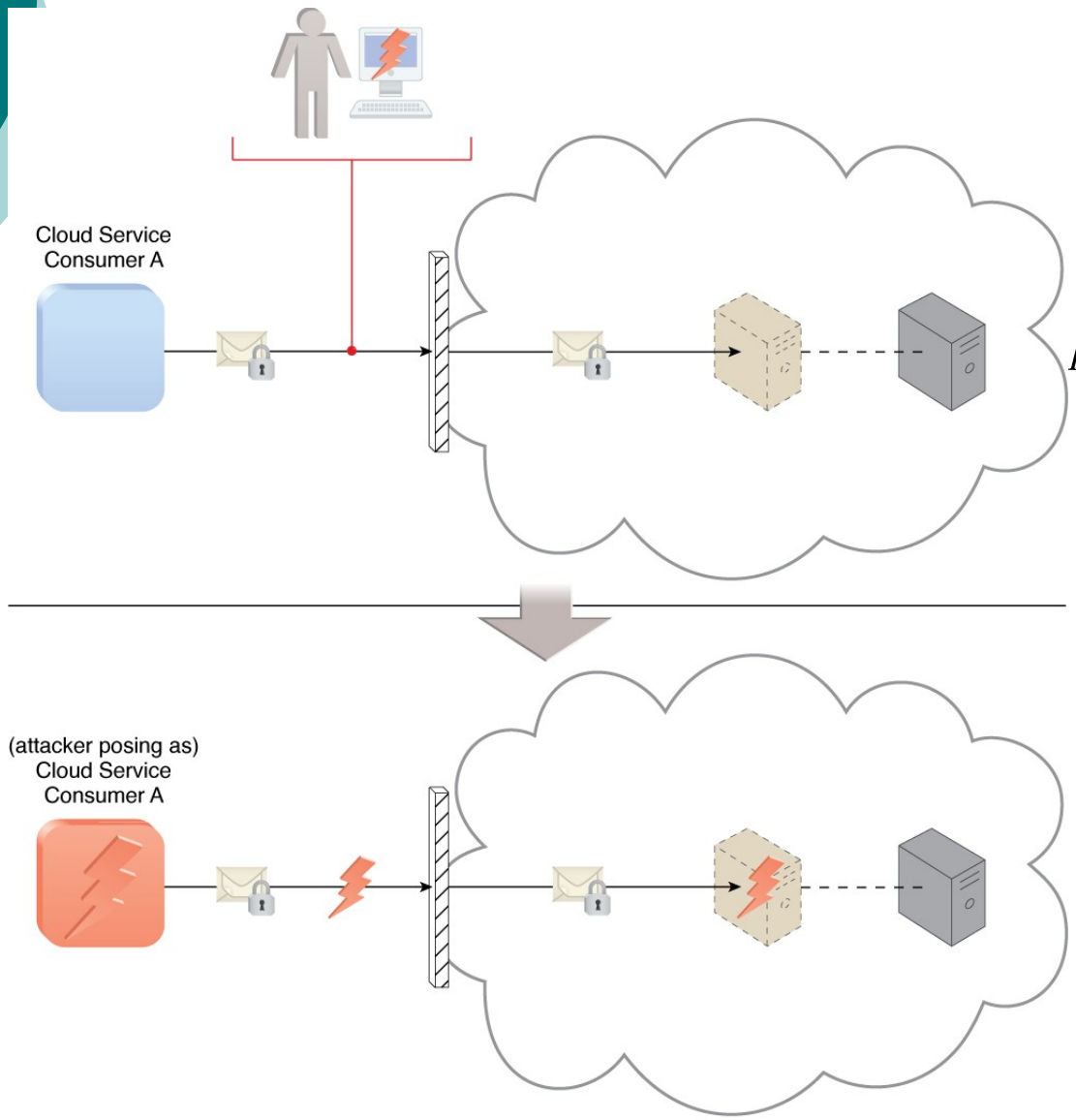


Figure 6.12 – An attacker has cracked a weak password used by Cloud Service Consumer A. As a result, a malicious cloud service consumer (owned by the attacker) is designed to pose as Cloud Service Consumer A in order to gain access to the cloud-based virtual server.

虚拟化攻击

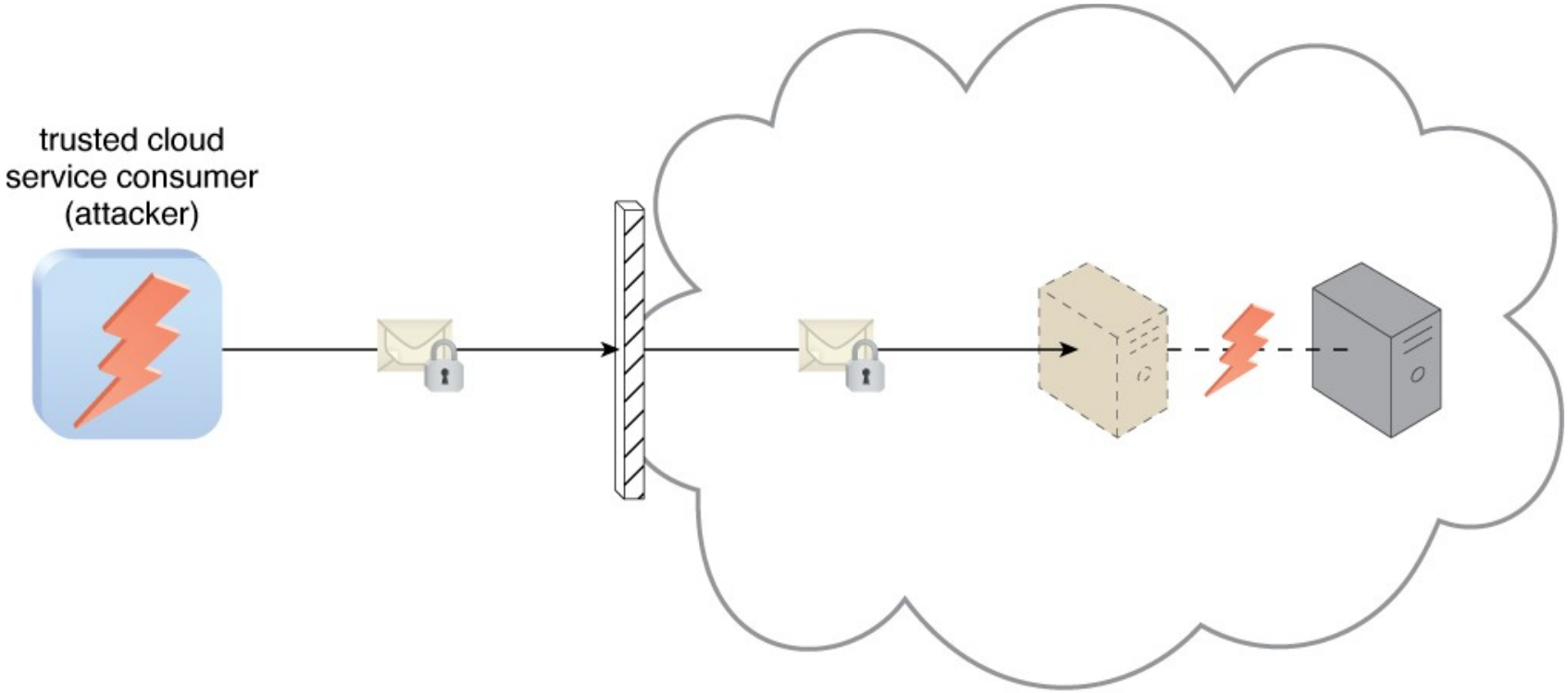


Figure 6.13 – An authorized cloud service consumer carries out a virtualization attack by abusing its administrative access to a virtual server to exploit the underlying hardware.

信任边界重叠

- 如果云中的物理IT资源是由不同的云服务用户共享的，那么这些云服务用户的信任边界是重叠的(Overlapping Trust Boundaries)。

- 恶意的云服务用户可以把目标设定为共享的IT资源，意图损害其他共享同样信任边界的云服务用户或IT资源。

信任边界重叠

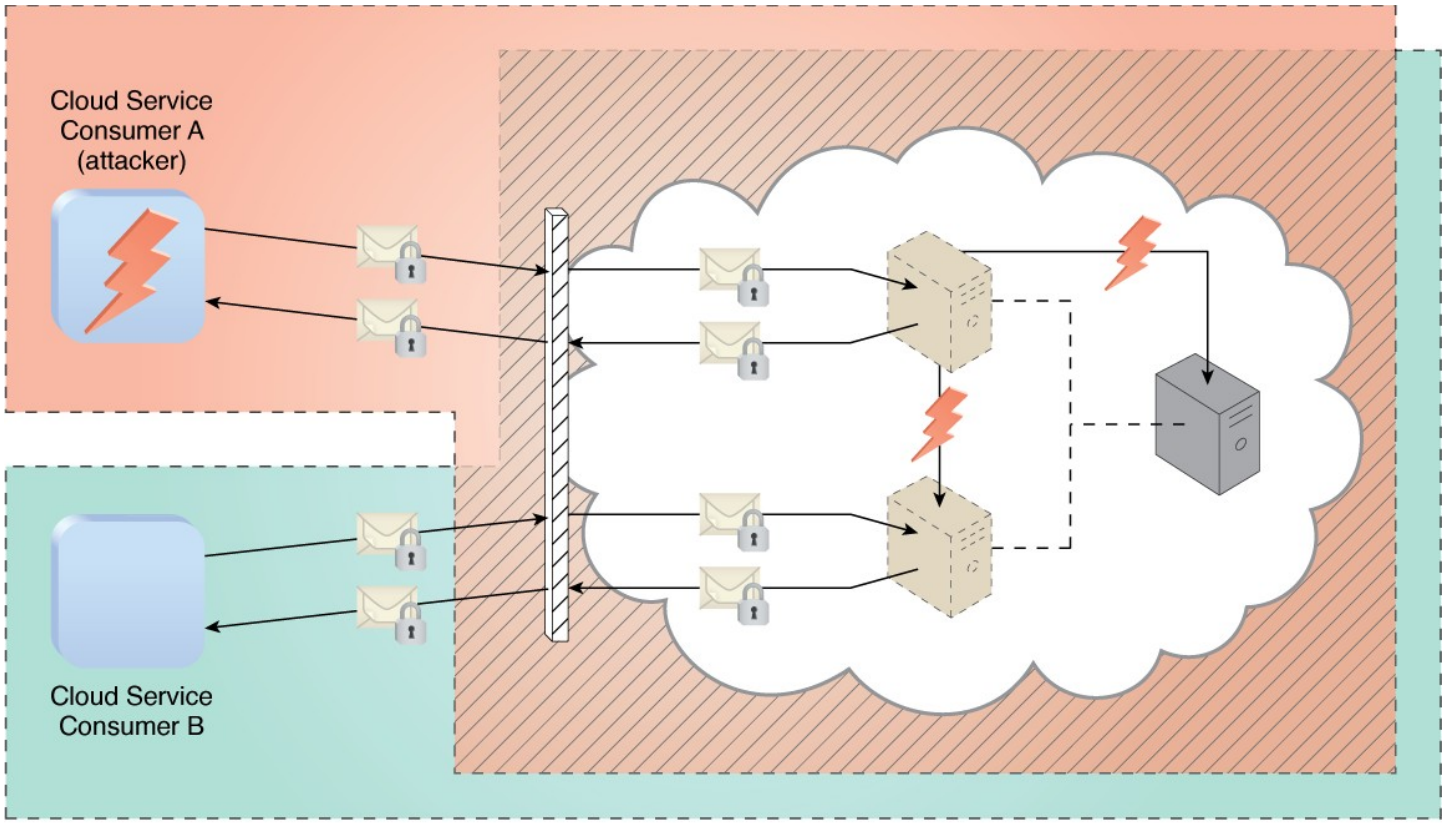


Figure 6.14 – Cloud Service Consumer A is trusted by the cloud and therefore gains access to its virtual server which it then attacks with the intention of attacking the underlying physical server and the virtual server used by Cloud Service Consumer B.

关键点小结

- 流量窃听和恶意媒介攻击通常是由截取网络流量的恶意服务作用者实施的，后者还进一步攥改。
- 拒绝服务攻击的发生是当目标IT资源由于请求过多而负载过重，这些请求意在使IT资源性能陷于瘫痪或不可用。
- 授权不足攻击是指错误地授予了攻击者访问权限或是授权太宽泛，或是是用了弱密码。
- 虚拟化攻击利用的是虚拟化环境中的漏洞，获得了对底层物理硬件未被授权的访问。
- 重叠的信任边界潜藏了一种威胁，攻击者可以利用多个云用户共享的、基于云的IT资源进行攻击。

其他考量

- 有缺陷的实现(Flawed Implementations)
  - 如果云提供者的软件或硬件有内在的安全缺陷或操作弱点：

1. 攻击者便会利用这些漏洞来损害云提供者的软件或硬件内在的安全缺陷或操作弱点。
2. 攻击者就会利用这些漏洞来损害云提供者的IT资源和由托管给云提供者的云用户的IT资源的完整性、保密性和可用性。

有缺陷的实现

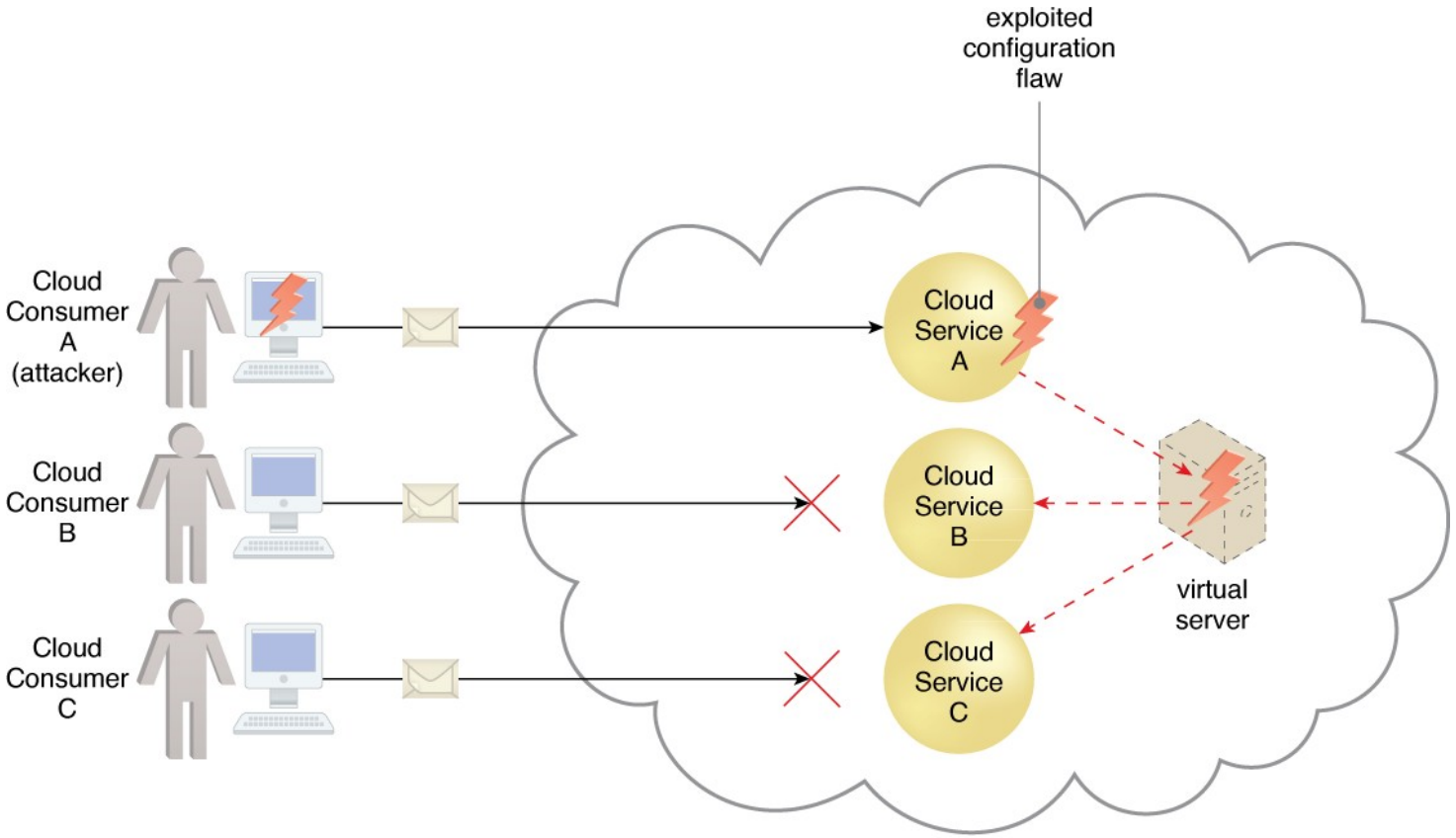


Figure 6.15 – Cloud Service Consumer A's message triggers a configuration flaw in Cloud Service A, which in turn causes the virtual server that is also hosting Cloud Services B and C to crash.

安全策略不一致与合约

- 安全策略不一致(Security Policy Disparity)
  - 云提供者提供的信息安全方法与传统的方法可能会不完全相同，甚至不相似。----云用户需要意识到，部署有缺陷的基于云的解决方案可能会引入安全风险

- 合约(Contracts)
  - 云用户需要很小心地检查云提供者提出的合约和SLA(Service-Level Agreement服务等级协议)，确保涉及资产安全的安全策略和其他相关的保障令人满意。

风险管理Risk Management

- 风险评估Risk Assessment
  - 在风险评估阶段，要分析云环境，识别出威胁可能会利用的潜在的漏洞和缺陷。
- 风险处理Risk Treatment
  - 风险减轻策略
  - 风险减轻行动
- 风险控制Risk Control
  - 考察、回顾相关的事件，决定之前的评估和对应的措施是不是有效的，确认是否要进行策略的调整。

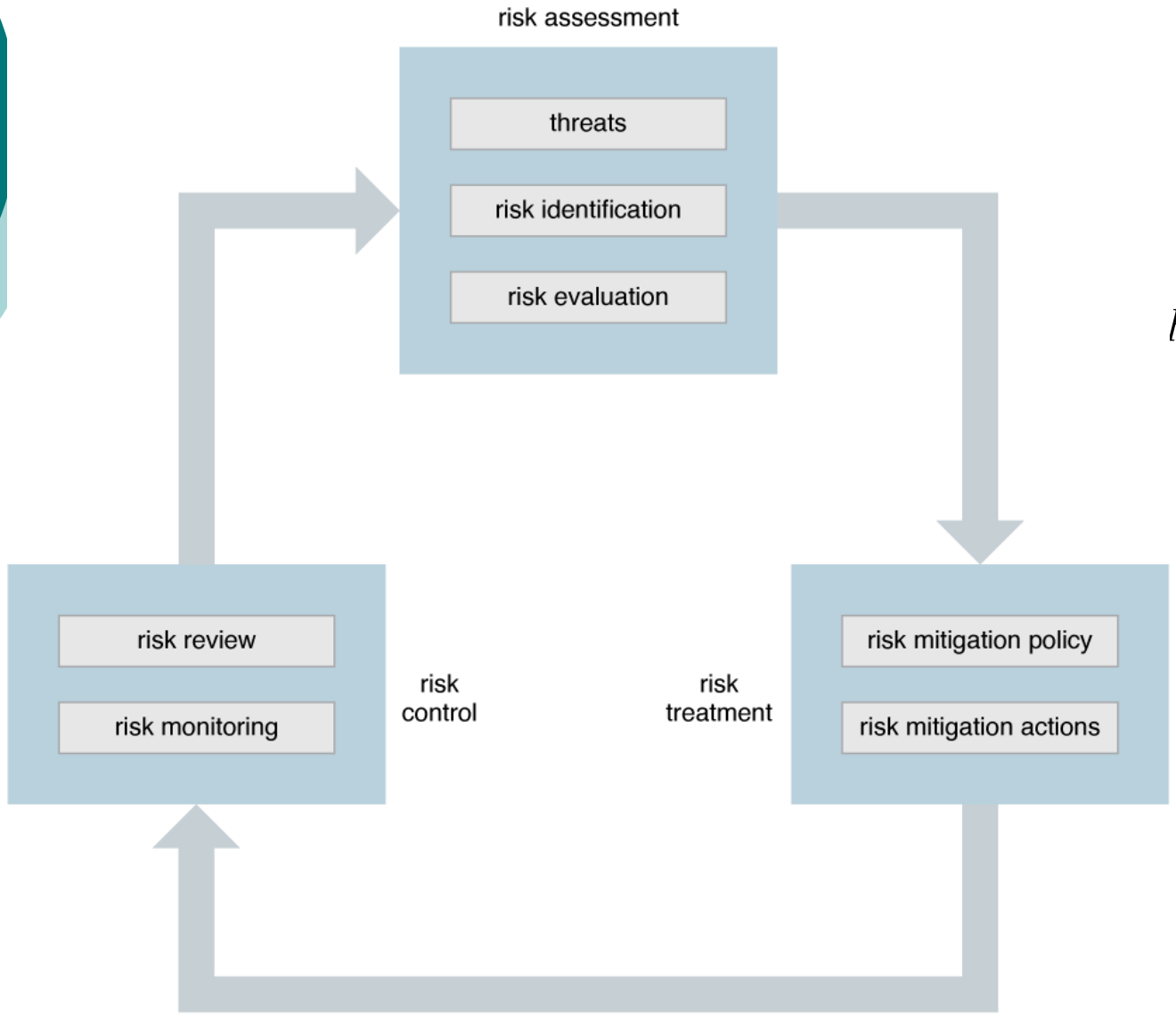


Figure 6.16 – The ongoing risk management process, which can be initiated from any of the three stages.

关键点小结

- 云用户需要意识到，部署有缺陷的基于云的解决方案可能会引入安全风险---这个安全风险是不同于传统风险的。
- 在选择云提供厂商时，理解云提供者如何定义和强加所有权，以及可能的不兼容的云安全策略，是形成评估标准的关键部分。
- 在用户和云提供者签署的安全协议中，需要明确定义和相互理解对潜在的安全泄露的责任、免责和问责。
- 对于云用户来说，在理解具体针对谋个特定云环境的安全相关的可能的问题之后，对识别出的风险进行相应的评估是很重要的。

本章小结

- 云安全基本术语：保密性、完整性、真实性、可用性
- 威胁作用者：匿名攻击者、恶意服务作用者、授信的攻击者、恶意的内部人员
- 云安全威胁种类：流量窃听、恶意媒介、拒绝服务、授信不足、虚拟化攻击、信任边界重叠
- 其他的考量：有缺陷的实现、安全策略不一致、合约、风险管理

课后题

1、分析讨论几个不同的威胁作用者。

2、分析讨论云安全威胁中常见威胁的引发原因和目的