SERVICE TECHNOLOGY SERIES FROM THOMAS ERL

"This is a great book on the topic of cloud computing."
—**Kapil Bakshi,** Architecture and Strategy, Cisco Systems Inc.

"We will recommend this book to Oracle customers, partners, and users for their journey toward cloud computing."
—**Jürgen Kress,** Fusion Middleware Partner Adoption, Oracle EMEA

"A cloud computing book that will stand out and survive the test of time. . . . I highly recommend this book. . ."
—**Christoph Schittko,** Principal Technology Strategist & Cloud Solution Director, Microsoft Corp.

". . . a must-read for any IT professional interested in cloud computing."
—**Andre Tost,** Senior Technical Staff Member, IBM Software Group

Cloud Computing
Concepts, Technology & Architecture

by Top-Selling Author Thomas Erl
with Zaigham Mahmood and Ricardo Puttini

Foreword by Pamela J. Wise-Martinez,
Department of Energy, National Nuclear Security Administration
Contributions by Gustavo Azzolin, Amin Naserpour, Vinícius Pacheco, Matthias Ziegler
Contribution by Michaela Iorga, Ph.D., Senior Security Technical Lead for Cloud Computing, NIST


physical server
firewall
CPU
memory
network adapter
physical network device
connection ports or virtual switch
virtual desktops
hypervisor
virtualization platform
virtual server
virtual firewall
virtual network device
VIM
VI manager
live VM migration
router
core switch
top-of-rack switch
schema or data model
policy
general machine processable document
human readable document
ready-made environment
management system
remote administration system
actively processing
component or program
product, system or application
service agent
message queue
repository or storage device
shared storage
state data in memory
service with state data (stateful service)
repository with state data
grid service
service
service composition
service layer
service contract (chorded circle notation)
decoupled service contract
service inventory

Malicious Service Agent

A *malicious service agent* is able to intercept and forward the network traffic that flows within a cloud (Figure 6.5). It typically exists as a service agent (or a program pretending to be a service agent) with compromised or malicious logic. It may also exist as an external program able to remotely intercept and potentially corrupt message contents.

Figure 6.5
The notation used for a malicious service agent.

Trusted Attacker

A *trusted attacker* shares IT resources in the same cloud environment as the cloud consumer and attempts to exploit legitimate credentials to target cloud providers and the cloud tenants with whom they share IT resources (Figure 6.6). Unlike anonymous attackers (which are non-trusted), trusted attackers usually launch their attacks from within a cloud's trust boundaries by abusing legitimate credentials or via the appropriation of sensitive and confidential information.

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

Trusted attackers (also known as *malicious tenants*) can use cloud-based IT resources for a wide range of exploitations, including the hacking of weak authentication processes, the breaking of encryption, the spamming of e-mail accounts, or to launch common attacks, such as denial of service campaigns.

Malicious Insider

Malicious insiders are human threat agents acting on behalf of or in relation to the cloud provider. They are typically current or former employees or third parties with access to the cloud provider's premises. This type of threat agent carries tremendous damage potential, as the malicious insider may have administrative privileges for accessing cloud consumer IT resources.

NOTE

A notation used to represent a general form of human-driven attack is the workstation combined with a lightning bolt (Figure 6.7). This generic symbol does not imply a specific threat agent, only that an attack was initiated via a workstation.

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

SUMMARY OF KEY POINTS

- An anonymous attacker is a non-trusted threat agent that usually attempts attacks from outside of a cloud's boundary.
- A malicious service agent intercepts network communication in an attempt to maliciously use or augment the data.
- A trusted attacker exists as an authorized cloud service consumer with legitimate credentials that it uses to exploit access to cloud-based IT resources.
- A malicious insider is a human that attempts to abuse access privileges to cloud premises.

6.3 Cloud Security Threats

This section introduces several common threats and vulnerabilities in cloud-based environments and describes the roles of the aforementioned threat agents. Security mechanisms that are used to counter these threats are covered in Chapter 10.

Traffic Eavesdropping

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). The aim of this attack is to directly compromise the confidentiality of the data and, possibly, the confidentiality of the relationship between the cloud consumer and cloud provider. Because of the passive nature of the attack, it can more easily go undetected for extended periods of time.

Malicious Intermediary

The *malicious intermediary* threat arises when messages are intercepted and altered by a malicious service agent, thereby potentially compromising the message's confidentiality and/or integrity. It may also insert harmful data into the message before forwarding it to its destination. Figure 6.9 illustrates a common example of the malicious intermediary attack.

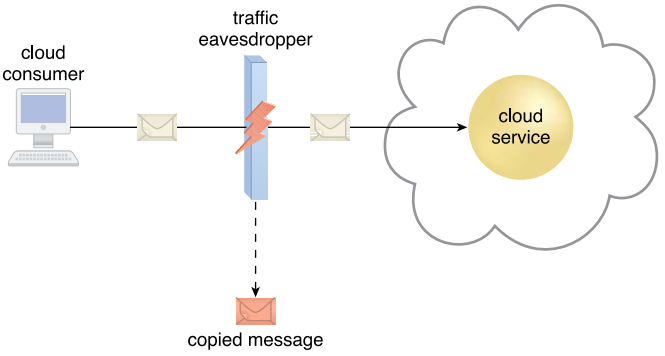

Figure 6.8
An externally positioned malicious service agent carries out a traffic eavesdropping attack by intercepting a message sent by the cloud service consumer to the cloud service. The service agent makes an unauthorized copy of the message before it is sent along its original path to the cloud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

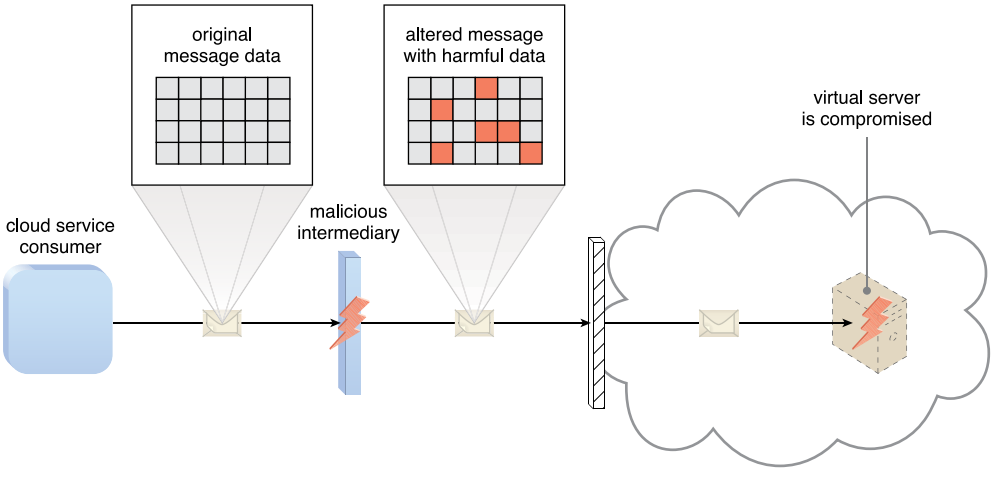

Figure 6.9
The malicious service agent intercepts and modifies a message sent by a cloud service consumer to a cloud service (not shown) being hosted on a virtual server. Because harmful data is packaged into the message, the virtual server is compromised.

NOTE

While not as common, the malicious intermediary attack can also be carried out by a malicious cloud service consumer program.

Denial of Service

The objective of the denial of service (DoS) attack is to overload IT resources to the point where they cannot function properly. This form of attack is commonly launched in one of the following ways:

- 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.

Successful DoS attacks produce server degradation and/or failure, as illustrated in Figure 6.10.

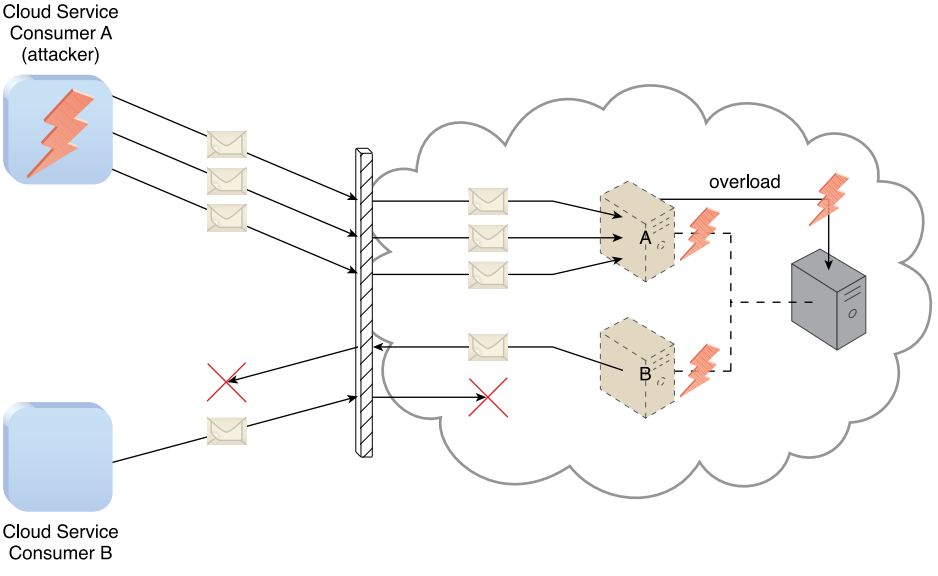

Figure 6.10

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.

Insufficient Authorization

The insufficient authorization attack 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. This is often a result of the attacker gaining direct access to IT resources that were implemented under the assumption that they would only be accessed by trusted consumer programs (Figure 6.11).

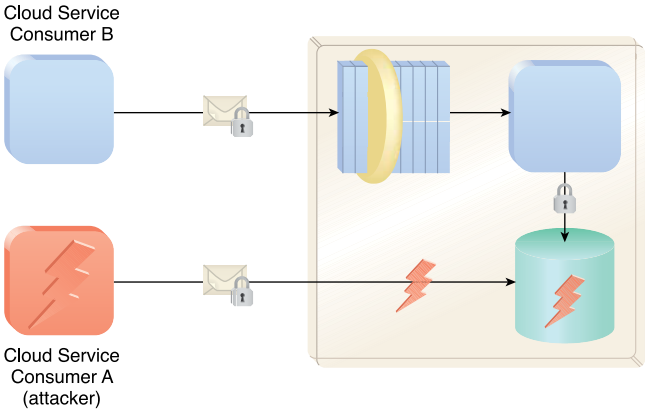

Figure 6.11
Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B).

A variation of this attack, known as *weak authentication*, can result when weak passwords or shared accounts are used to protect IT resources. Within cloud environments, these types of attacks can lead to significant impacts depending on the range of IT resources and the range of access to those IT resources the attacker gains (Figure 6.12).

Virtualization Attack

Virtualization provides multiple cloud consumers with access to IT resources that share underlying hardware but are logically isolated from each other. Because cloud providers grant cloud consumers administrative access to virtualized IT resources (such as virtual servers), there is an inherent risk that cloud consumers could abuse this access to attack the underlying physical IT resources.

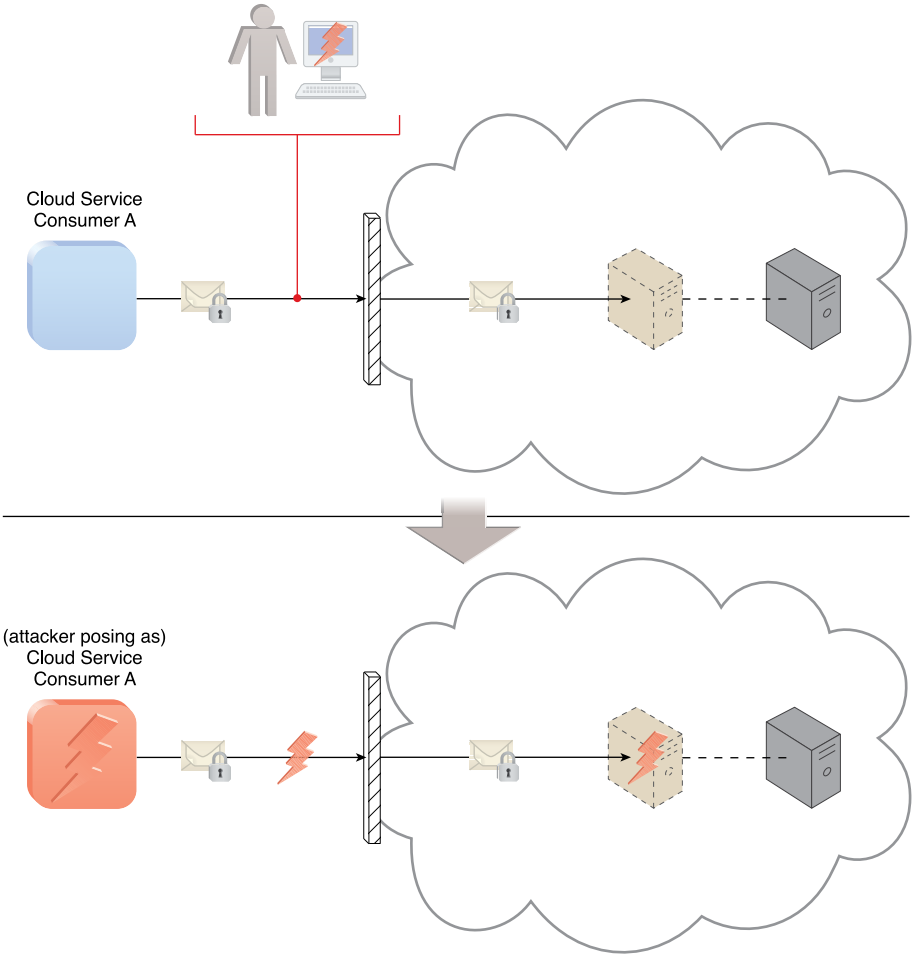

Figure 6.12

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.