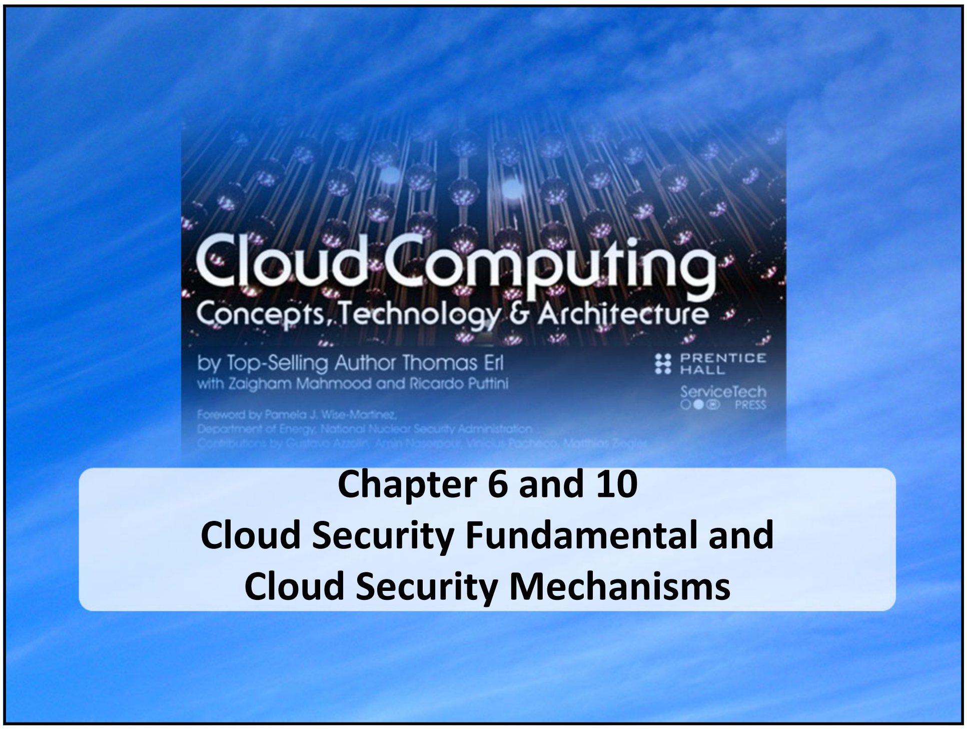


Cloud Computing

Concepts, Technology & Architecture

by Top-Selling Author Thomas Erl

with Zaigham Mahmood and Ricardo Puttini

PRENTICE HALL

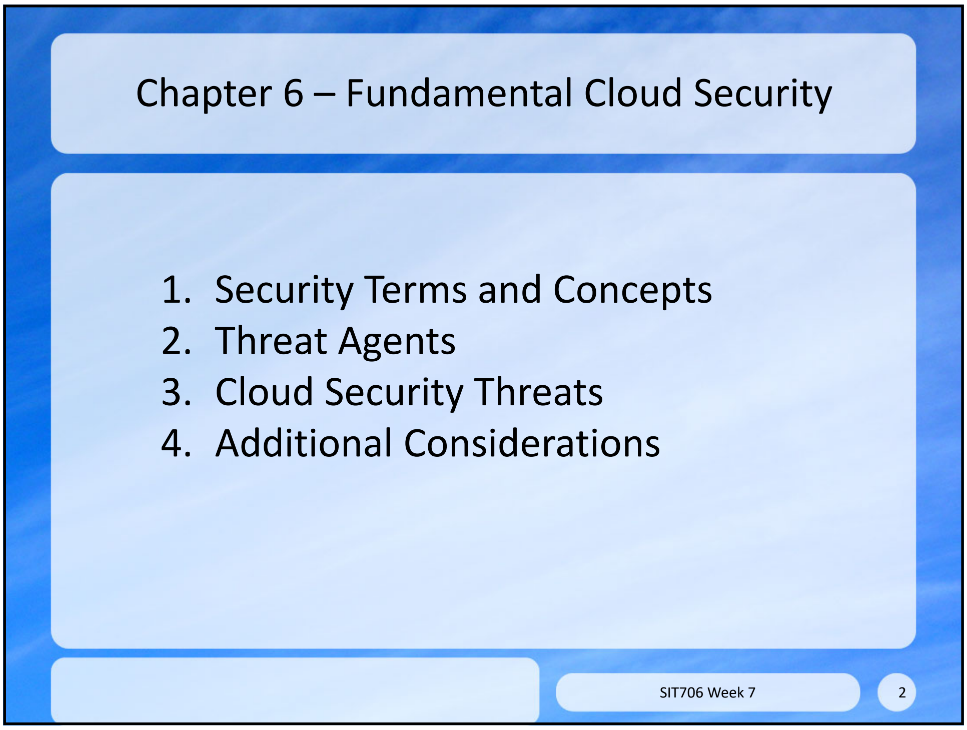
ServiceTech PRESS

Foreword by Pamela J. Wise-Martinez,

Department of Energy, National Nuclear Security Administration

Contributions by Gustavo Azzolin, Amin Naserpour, Vinicius Pacheco, Matthias Ziegler

Chapter 6 and 10
Cloud Security Fundamental and
Cloud Security Mechanisms



Chapter 6 – Fundamental Cloud Security

1. Security Terms and Concepts
2. Threat Agents
3. Cloud Security Threats
4. Additional Considerations

SIT706 Week 7 2

Security Terms and Concepts

- Confidentiality: data accessible only to authorised parties, restricting access in transit and storage.

- **Data confidentiality**
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- **Privacy**
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Security Terms and Concepts

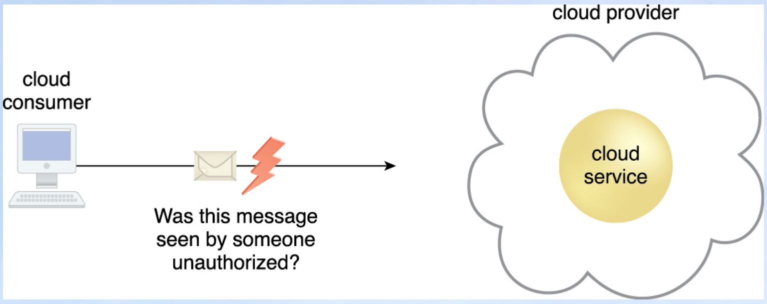


Figure 6.1 The message issued by the cloud consumer to the cloud service is considered confidential only if it is not accessed or read by an unauthorized party.

Security Terms and Concepts

- Integrity: not altered by an unauthorized party, guarantees that data transmitted to a cloud matches the data received/stored on cloud IT resources
- **Data integrity**
  - Assures that information and programs are changed only in a specified and authorized manner
- **System integrity**
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Security Terms and Concepts

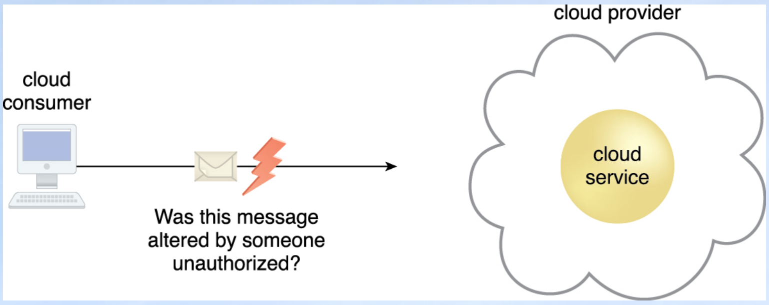
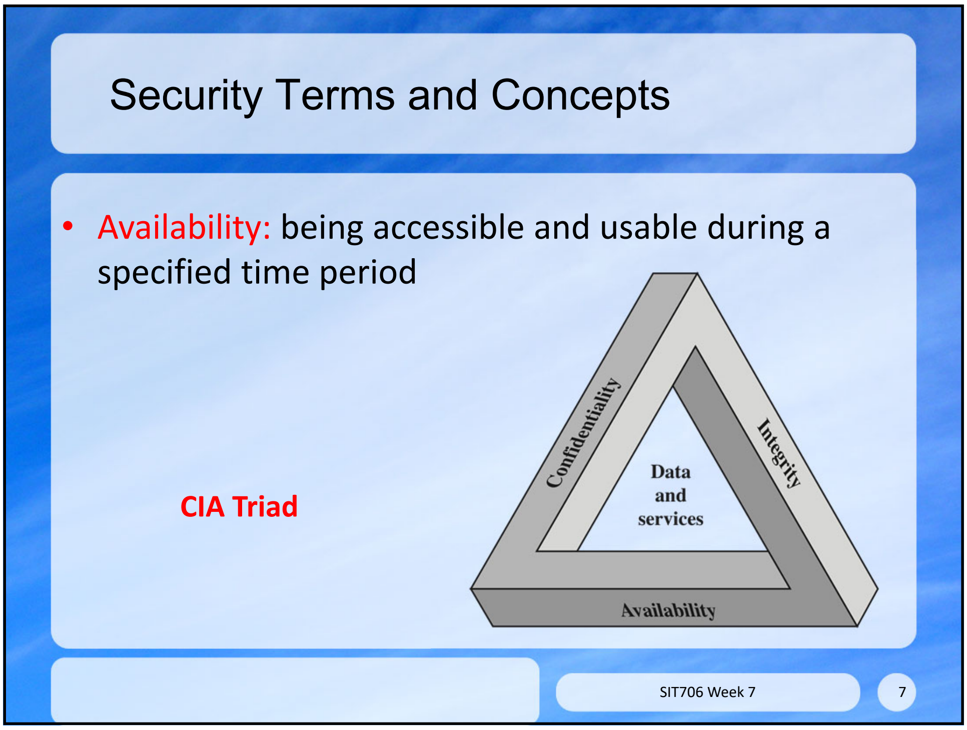


Figure 6.2 The message issued by the cloud consumer to the cloud service is considered to have integrity if it has not been altered.



Security Terms and Concepts

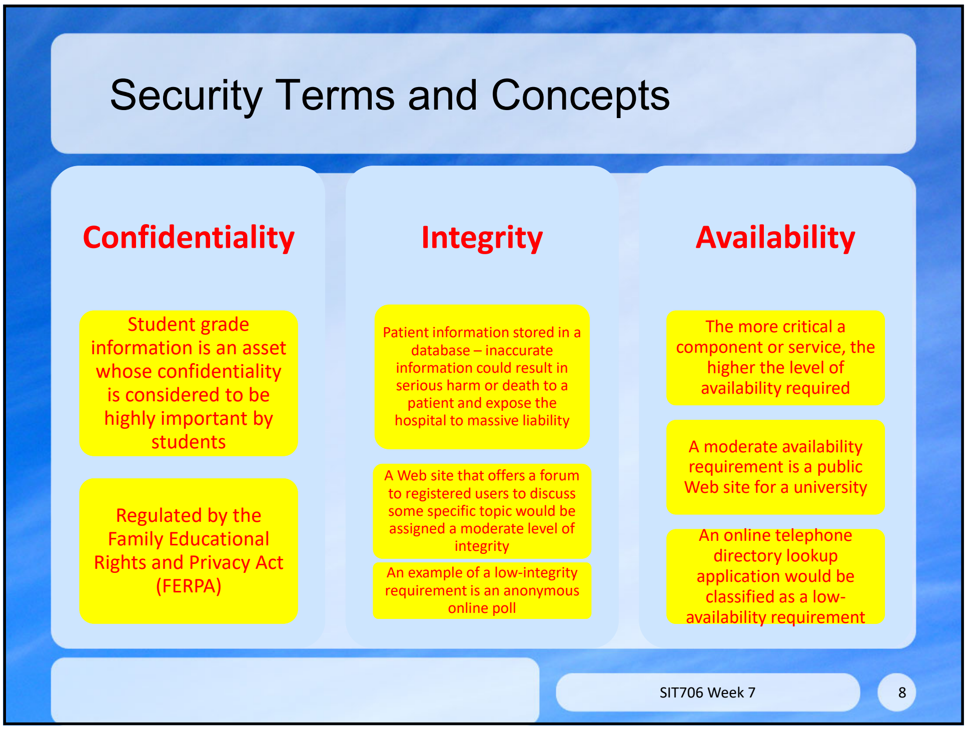
- Availability: being accessible and usable during a specified time period

CIA Triad

Confidentiality
Integrity
Availability
Data and services

SIT706 Week 7

7



Security Terms and Concepts

Confidentiality

Student grade information is an asset whose confidentiality is considered to be highly important by students

Regulated by the Family Educational Rights and Privacy Act (FERPA)

Integrity

Patient information stored in a database – inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability

A Web site that offers a forum to registered users to discuss some specific topic would be assigned a moderate level of integrity

An example of a low-integrity requirement is an anonymous online poll

Availability

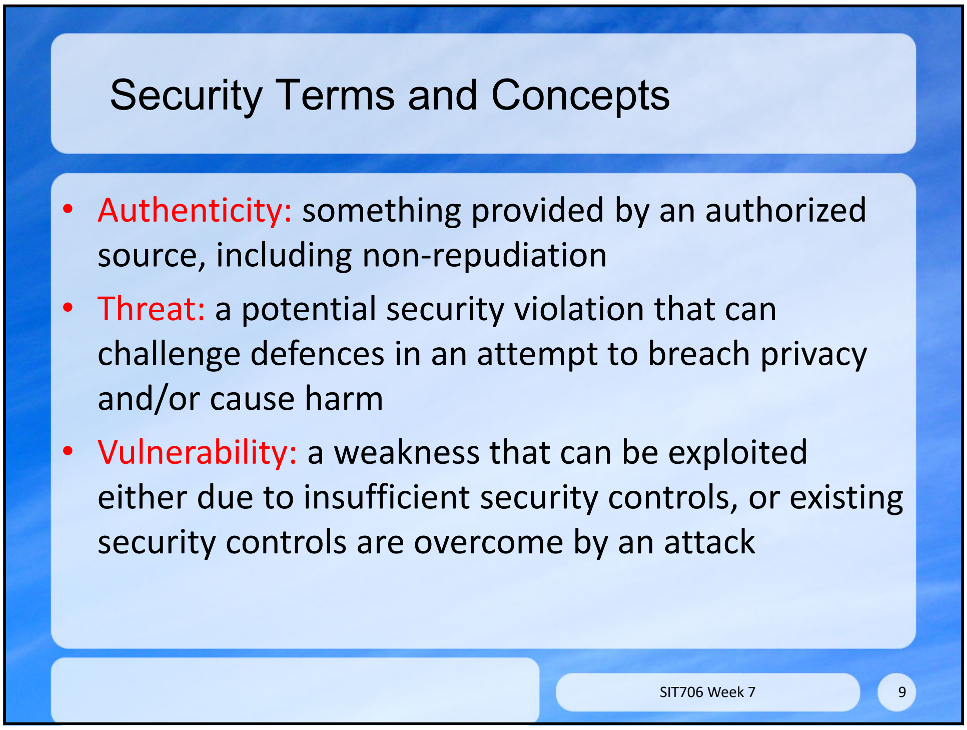
The more critical a component or service, the higher the level of availability required

A moderate availability requirement is a public Web site for a university

An online telephone directory lookup application would be classified as a low-availability requirement

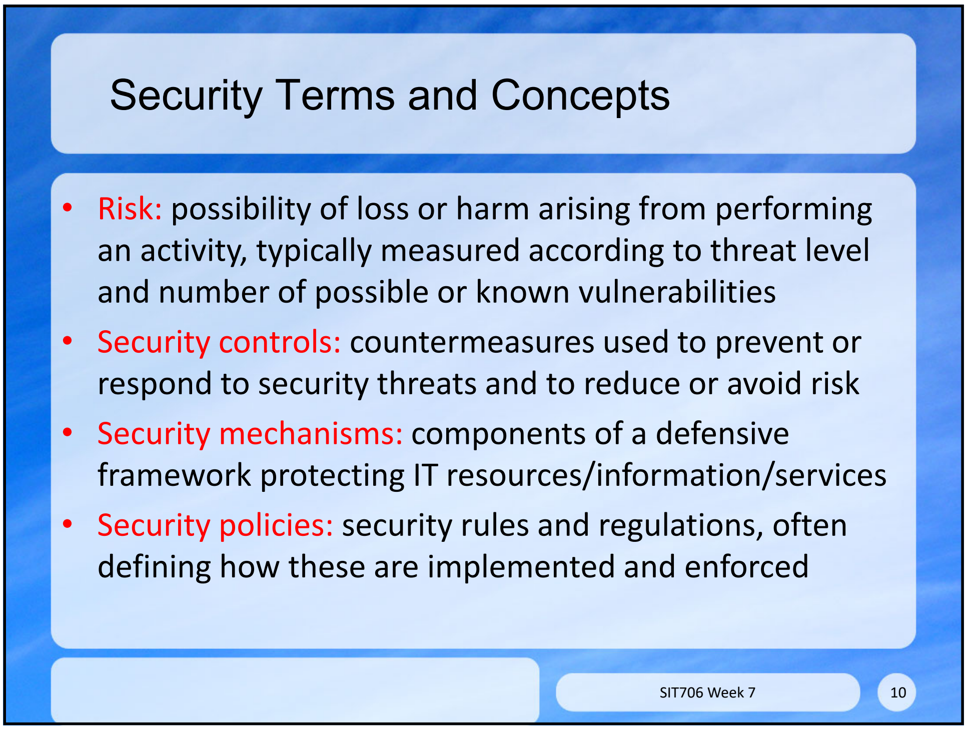
SIT706 Week 7

8



Security Terms and Concepts

- Authenticity: something provided by an authorized source, including non-repudiation
- Threat: a potential security violation that can challenge defences in an attempt to breach privacy and/or cause harm
- Vulnerability: a weakness that can be exploited either due to insufficient security controls, or existing security controls are overcome by an attack



Security Terms and Concepts

- Risk: possibility of loss or harm arising from performing an activity, typically measured according to threat level and number of possible or known vulnerabilities
- Security controls: countermeasures used to prevent or respond to security threats and to reduce or avoid risk
- Security mechanisms: components of a defensive framework protecting IT resources/information/services
- Security policies: security rules and regulations, often defining how these are implemented and enforced

Security Terms and Concepts

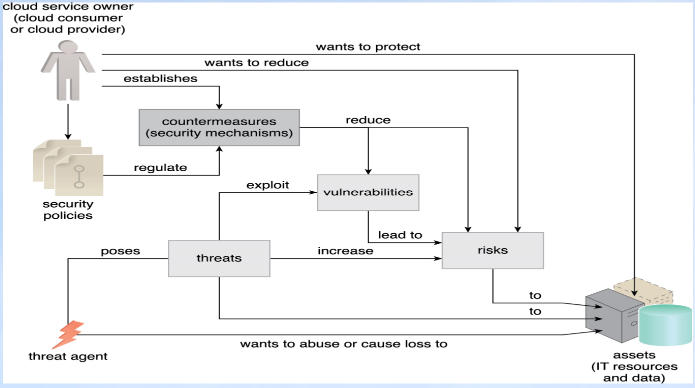
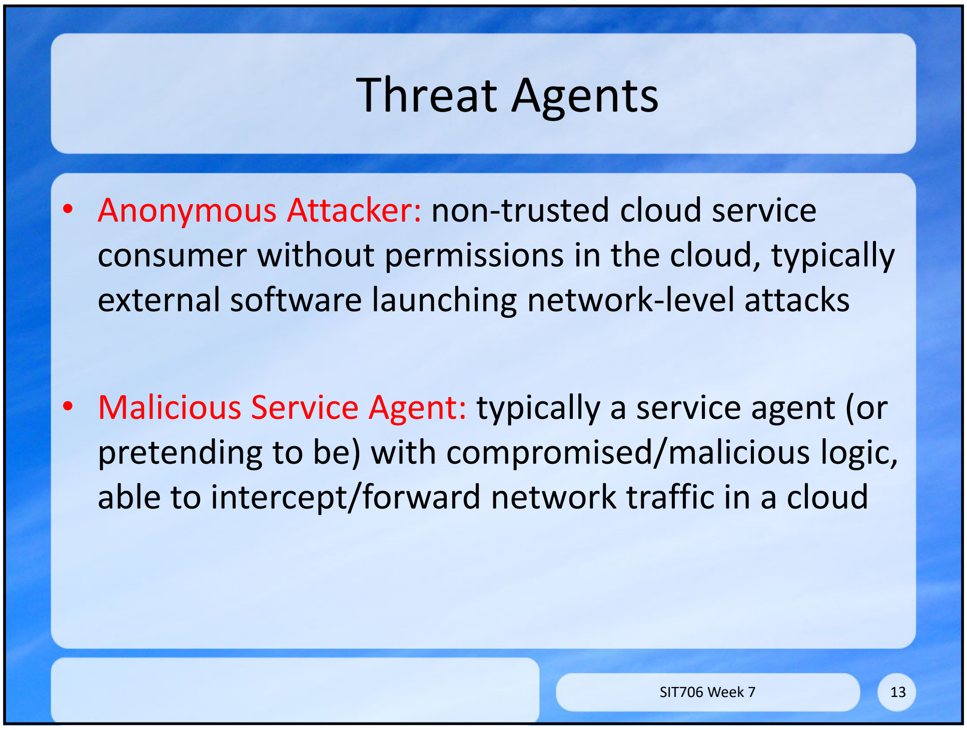


Figure 6.3 How security policies and security mechanisms are used to counter threats, vulnerabilities, and risks caused by threat agents.

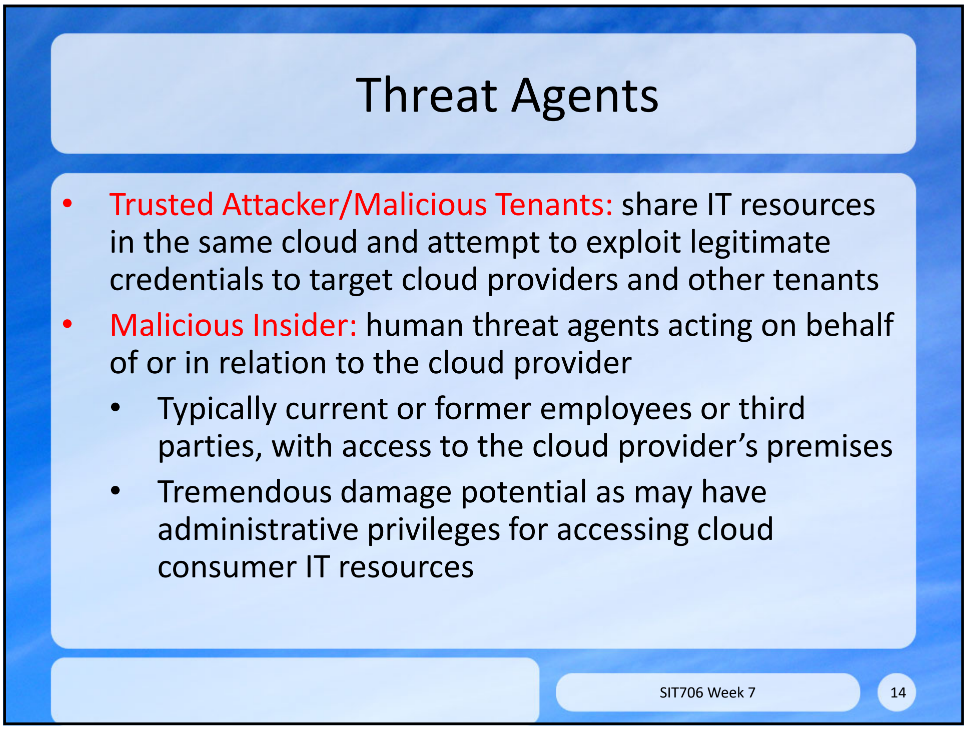
Threat Agents

- A threat agent is an entity posing a threat because it is capable of carrying out an attack; can be:
  - Either internal or external
  - Either from humans or software programs



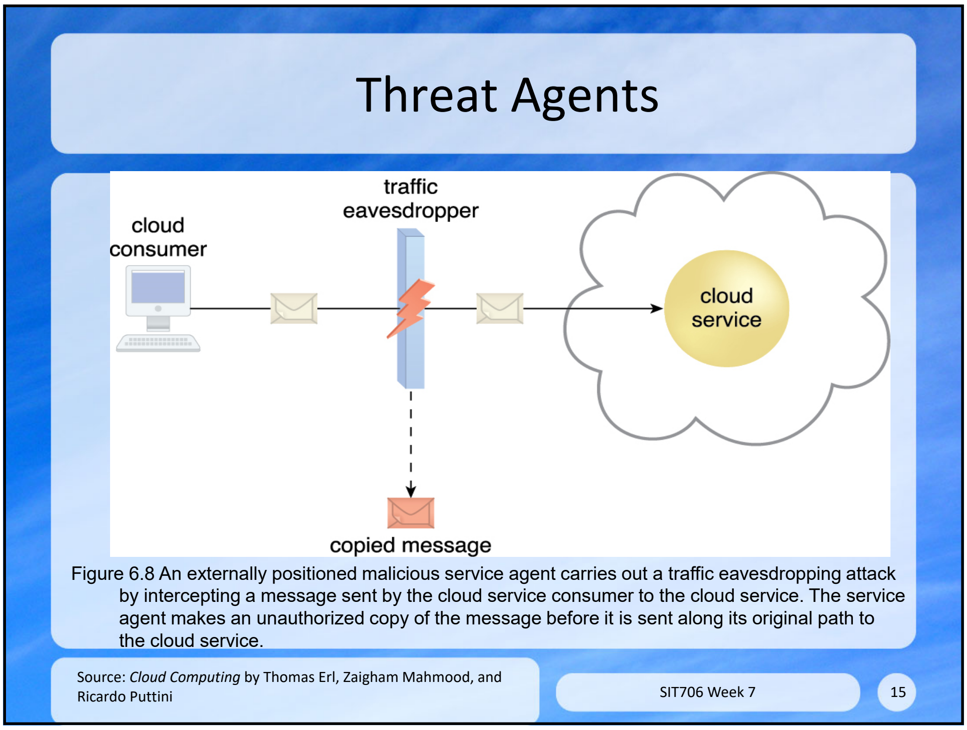
Threat Agents

- Anonymous Attacker: non-trusted cloud service consumer without permissions in the cloud, typically external software launching network-level attacks
- Malicious Service Agent: typically a service agent (or pretending to be) with compromised/malicious logic, able to intercept/forward network traffic in a cloud



Threat Agents

- Trusted Attacker/Malicious Tenants: share IT resources in the same cloud and attempt to exploit legitimate credentials to target cloud providers and other tenants
- 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
  - Tremendous damage potential as may have administrative privileges for accessing cloud consumer IT resources



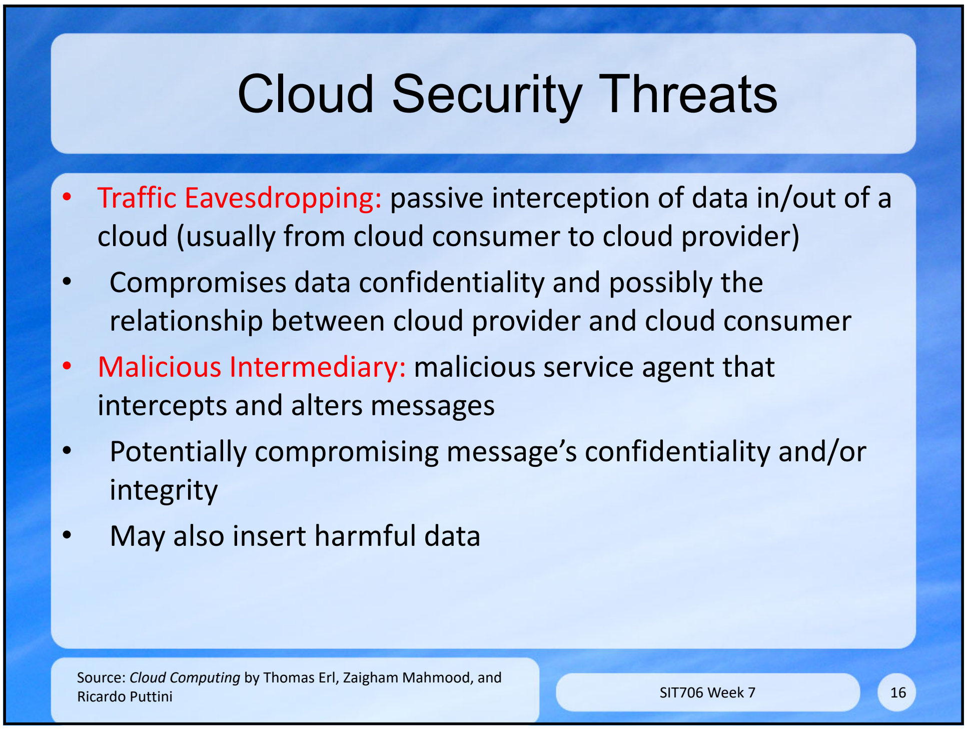
Threat Agents

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.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

15



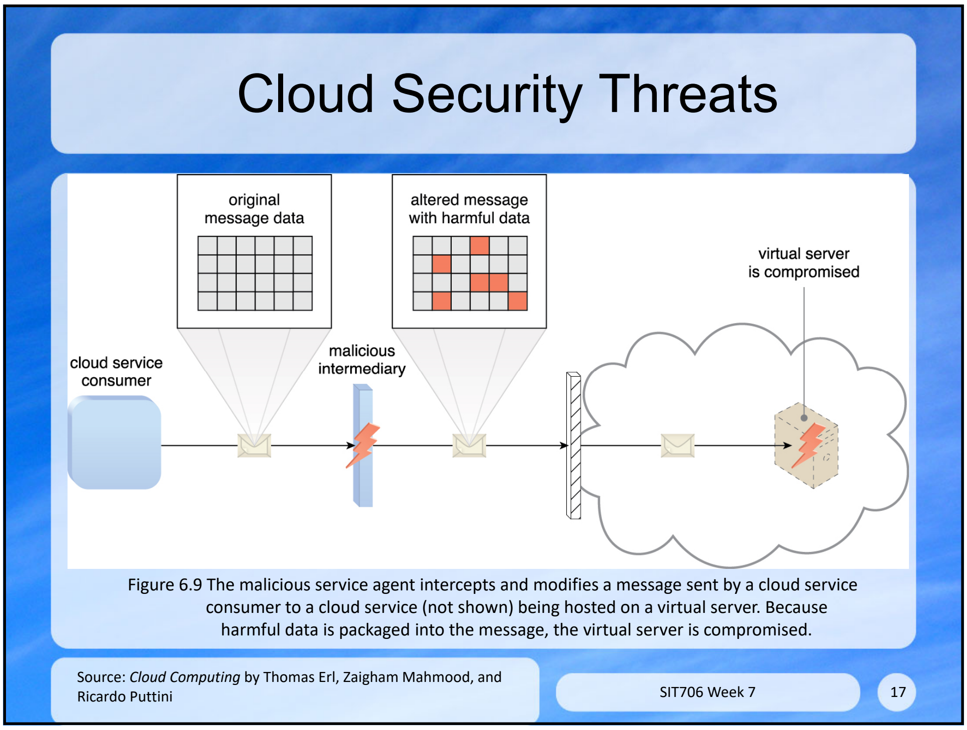
Cloud Security Threats

- Traffic Eavesdropping: passive interception of data in/out of a cloud (usually from cloud consumer to cloud provider)
- Compromises data confidentiality and possibly the relationship between cloud provider and cloud consumer
- Malicious Intermediary: malicious service agent that intercepts and alters messages
- Potentially compromising message’s confidentiality and/or integrity
- May also insert harmful data

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

16



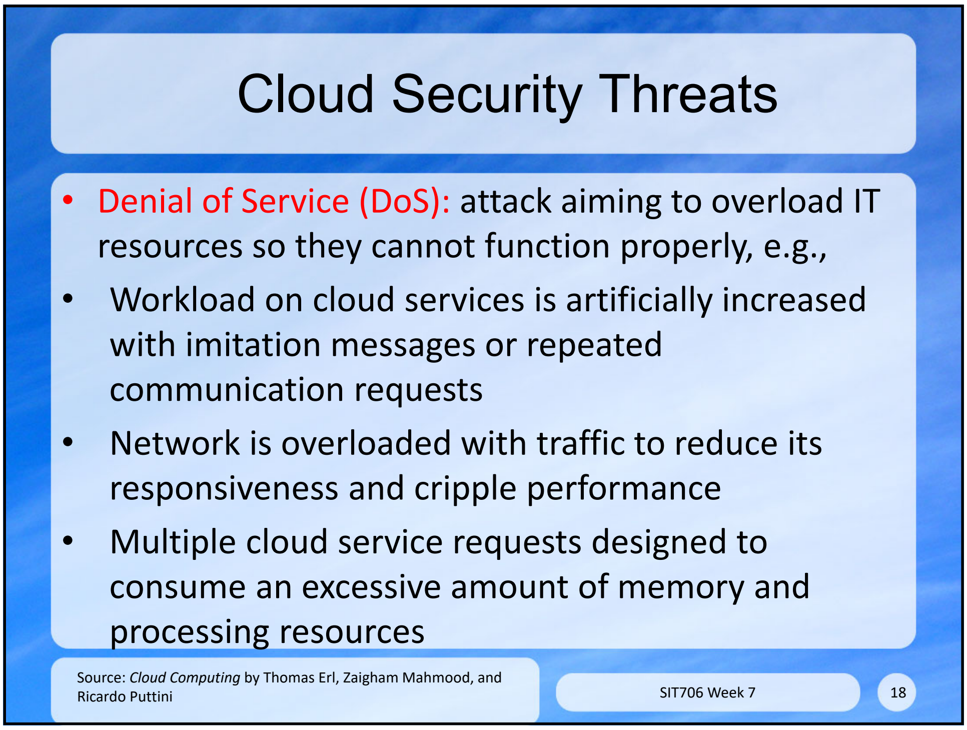
Cloud Security Threats

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.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

17



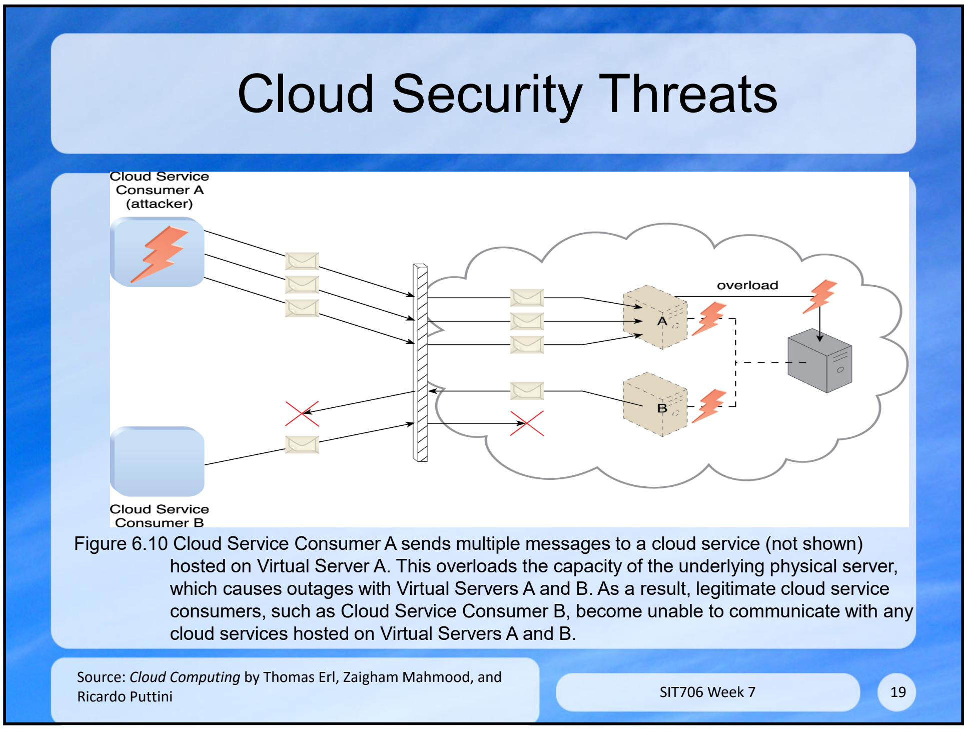
Cloud Security Threats

- Denial of Service (DoS): attack aiming to overload IT resources so they cannot function properly, e.g.,
- Workload on cloud services is artificially increased with imitation messages or repeated communication requests
- Network is overloaded with traffic to reduce its responsiveness and cripple performance
- Multiple cloud service requests designed to consume an excessive amount of memory and processing resources

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

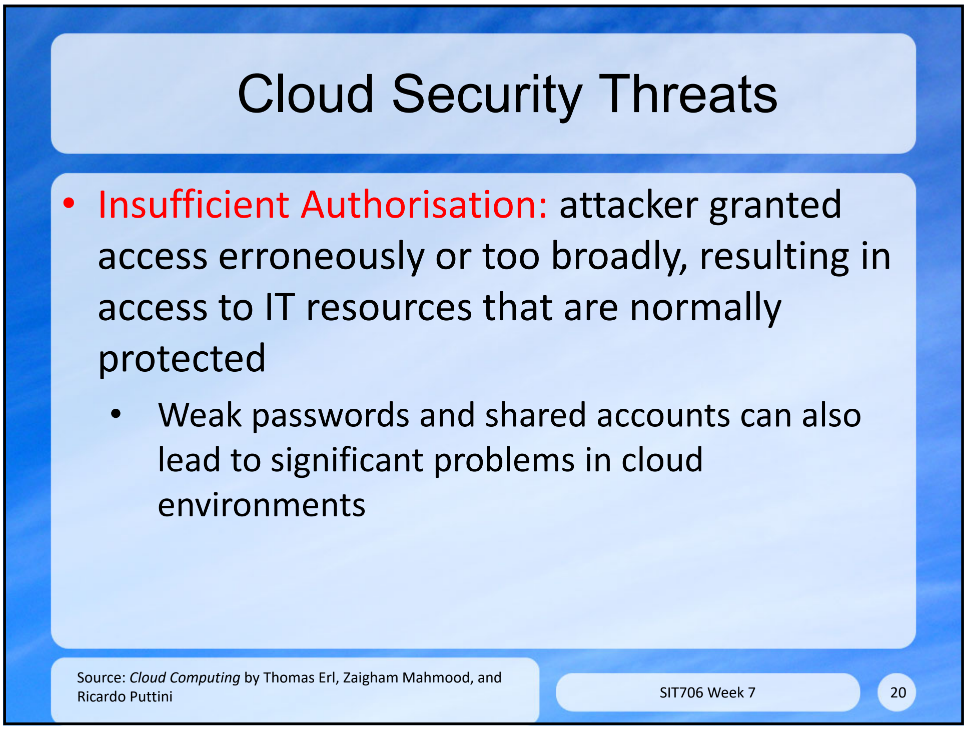
18



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.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



Cloud Security Threats

- Insufficient Authorisation: attacker granted access erroneously or too broadly, resulting in access to IT resources that are normally protected
    - Weak passwords and shared accounts can also lead to significant problems in cloud environments

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

Cloud Security Threats

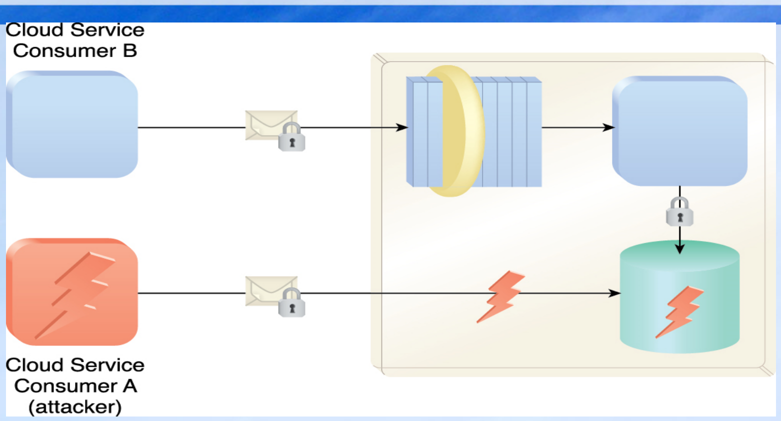
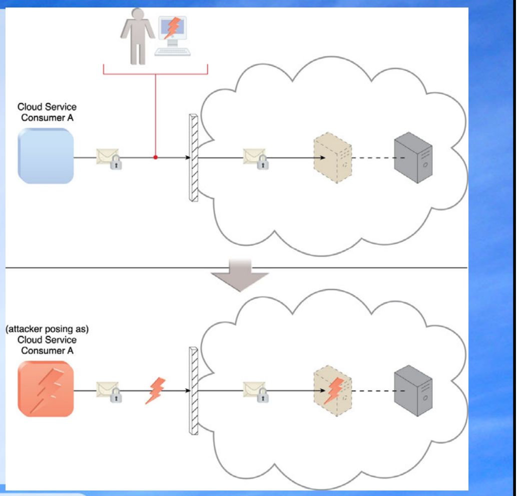


Figure 6.11 Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B).

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

Cloud Security Threats

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 Service Consumer B).



Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

Cloud Security Threats

- Virtualisation attack: multiple cloud consumers accessing shared hardware can enable one consumer to attack the underlying physical IT resources
  - Exploiting vulnerabilities in the virtualization platform to attack confidentiality, integrity, and/or availability

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

Cloud Security Threats

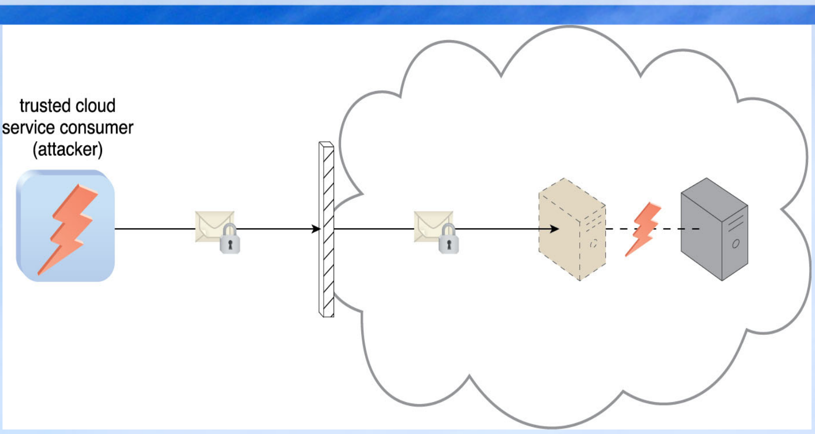
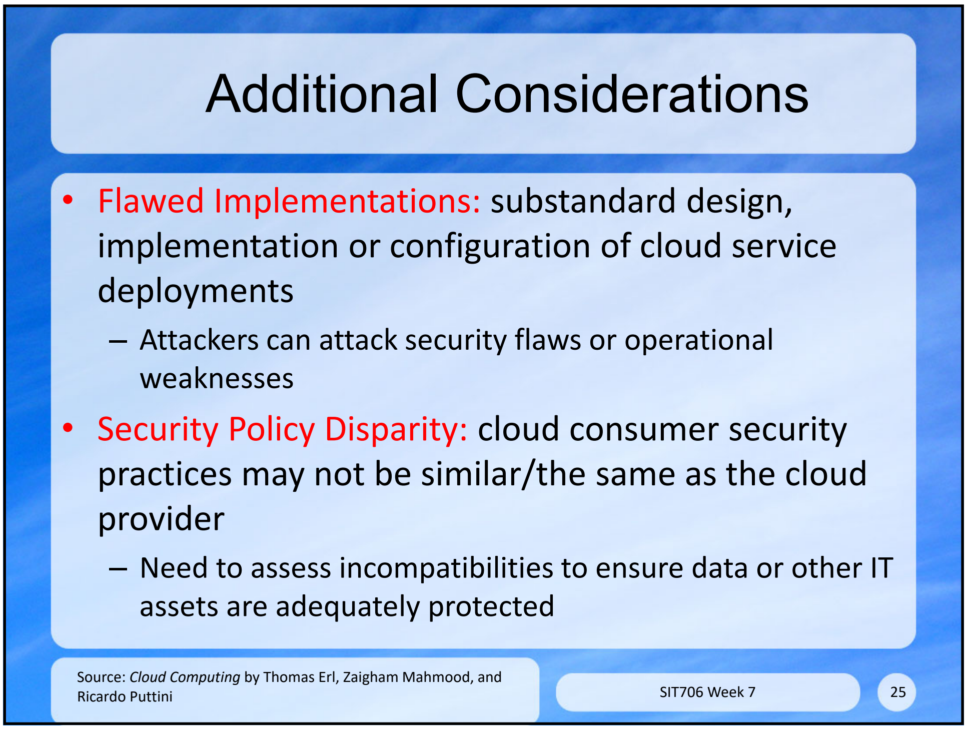


Figure 6.13 An authorized cloud service consumer carries out a virtualization attack by abusing its administrative access to a virtual server to exploit the underlying hardware.

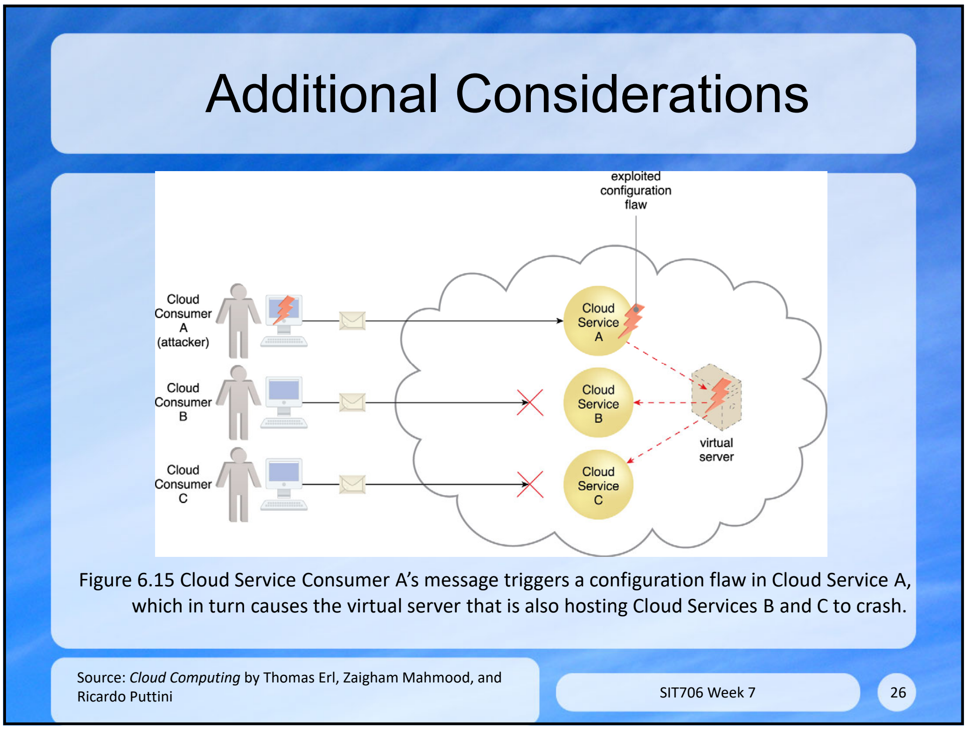
Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



Additional Considerations

- Flawed Implementations: substandard design, implementation or configuration of cloud service deployments
  - Attackers can attack security flaws or operational weaknesses
- Security Policy Disparity: cloud consumer security practices may not be similar/the same as the cloud provider
  - Need to assess incompatibilities to ensure data or other IT assets are adequately protected

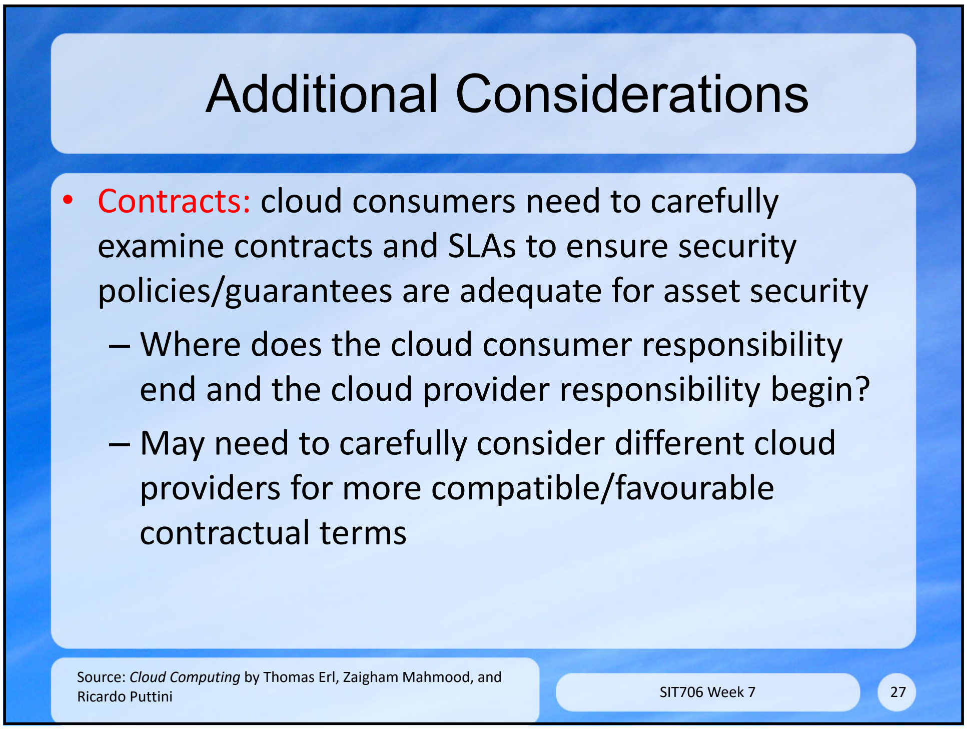
Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



Additional Considerations

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.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



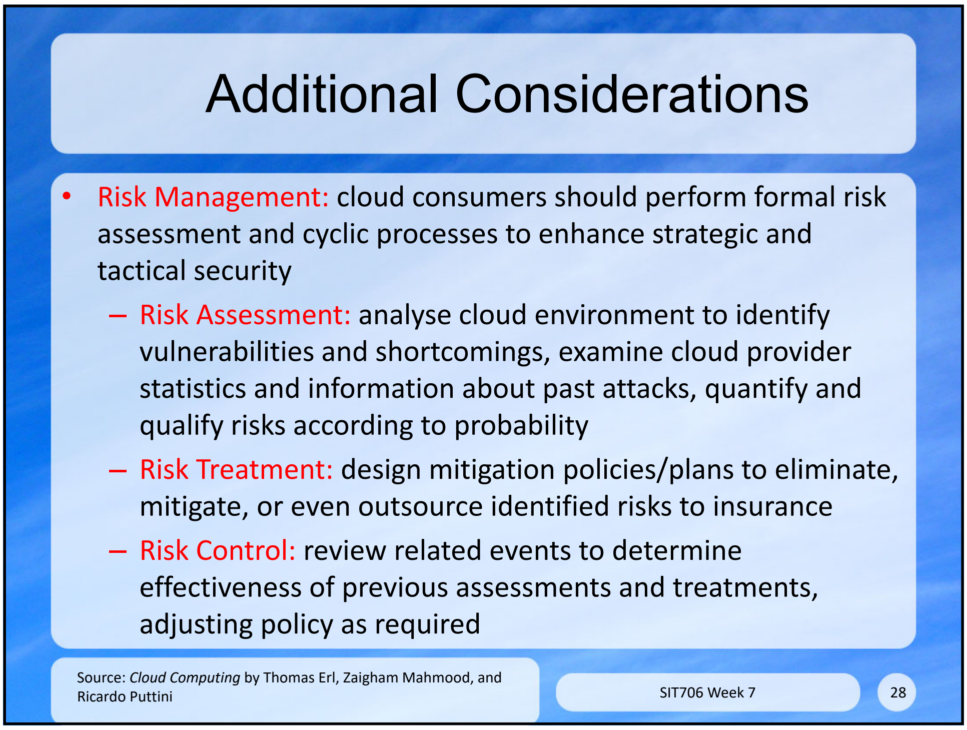
Additional Considerations

- Contracts: cloud consumers need to carefully examine contracts and SLAs to ensure security policies/guarantees are adequate for asset security
  - Where does the cloud consumer responsibility end and the cloud provider responsibility begin?
  - May need to carefully consider different cloud providers for more compatible/favourable contractual terms

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

27



Additional Considerations

- Risk Management: cloud consumers should perform formal risk assessment and cyclic processes to enhance strategic and tactical security
  - Risk Assessment: analyse cloud environment to identify vulnerabilities and shortcomings, examine cloud provider statistics and information about past attacks, quantify and qualify risks according to probability
  - Risk Treatment: design mitigation policies/plans to eliminate, mitigate, or even outsource identified risks to insurance
  - Risk Control: review related events to determine effectiveness of previous assessments and treatments, adjusting policy as required

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

28

Additional Considerations

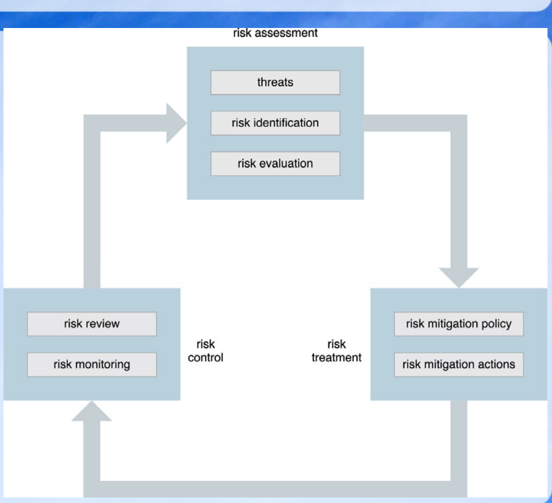


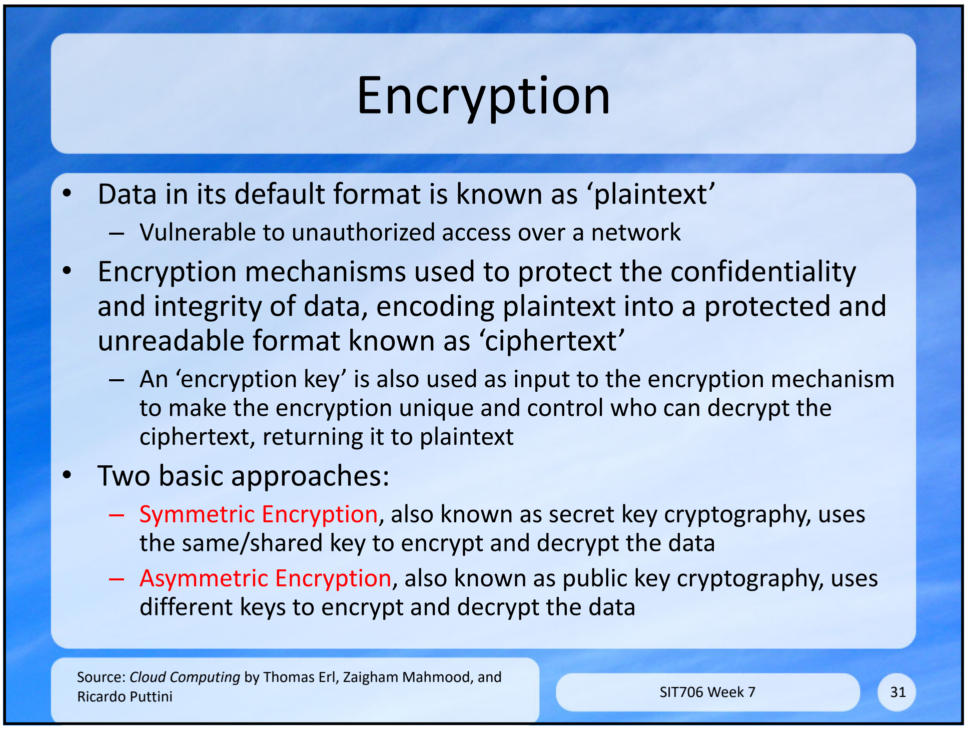
Figure 6.16 The on-going risk management process, which can be initiated from any of the three stages.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

Chapter 10 – Cloud Security Mechanisms

1. Encryption
2. Hashing
3. Digital Signature
4. Public Key Infrastructure (PKI)
5. Identity and Access Management (IAM)
6. Single Sign-On (SSO)
7. Cloud-Based Security Groups
8. Hardened Virtual Server Images

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



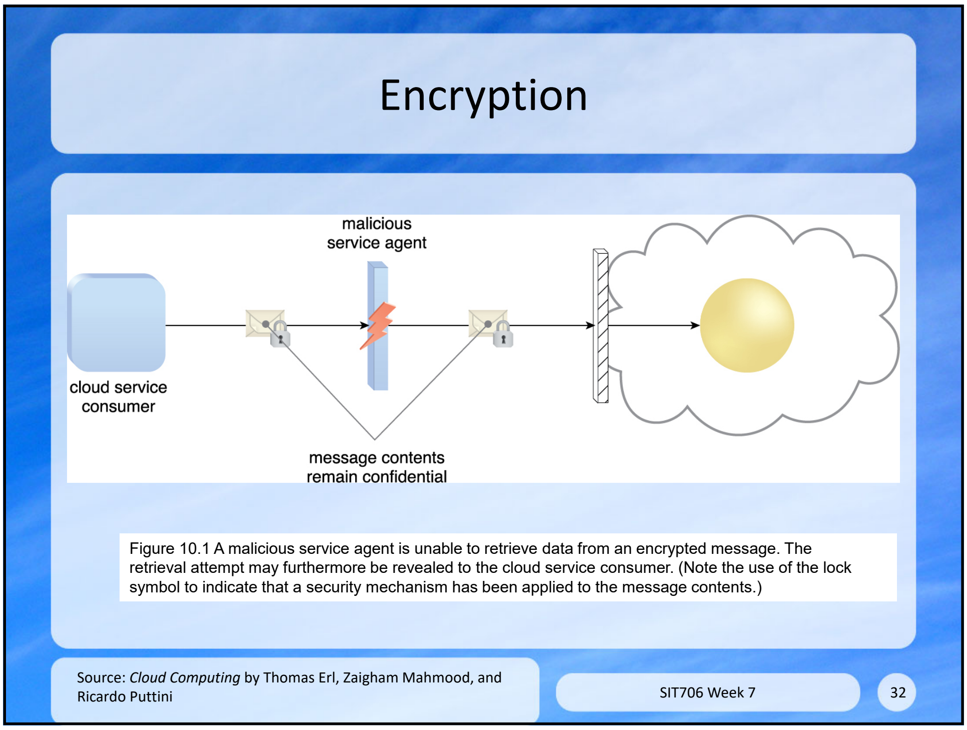
Encryption

- Data in its default format is known as ‘plaintext’
  - Vulnerable to unauthorized access over a network
- Encryption mechanisms used to protect the confidentiality and integrity of data, encoding plaintext into a protected and unreadable format known as ‘ciphertext’
  - An ‘encryption key’ is also used as input to the encryption mechanism to make the encryption unique and control who can decrypt the ciphertext, returning it to plaintext
- Two basic approaches:
  - Symmetric Encryption, also known as secret key cryptography, uses the same/shared key to encrypt and decrypt the data
  - Asymmetric Encryption, also known as public key cryptography, uses different keys to encrypt and decrypt the data

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

31



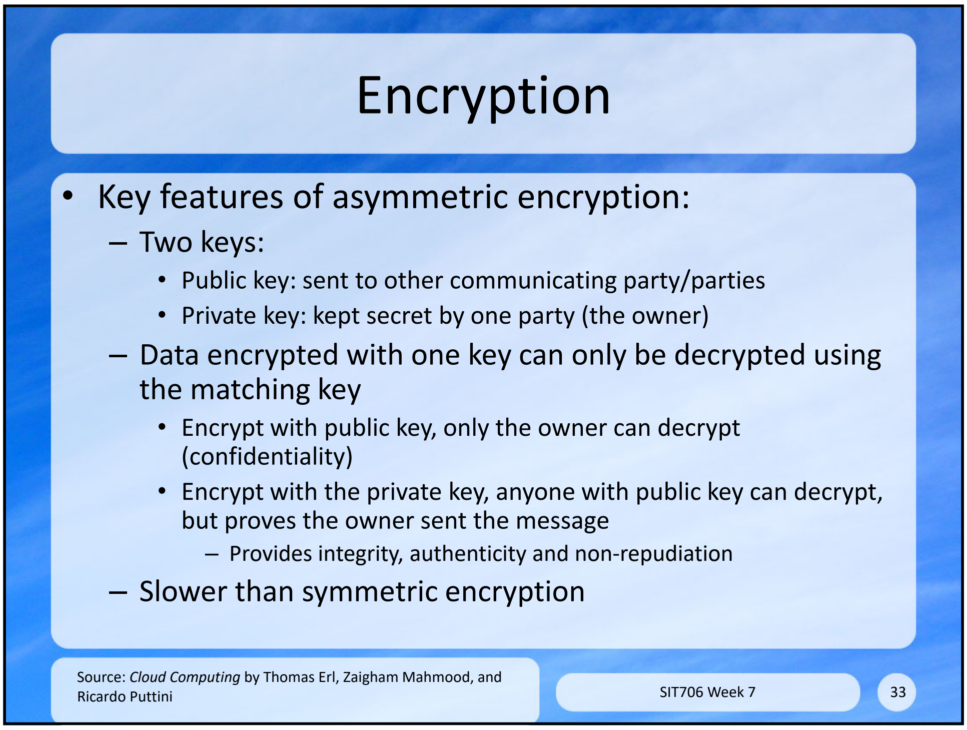
Encryption

Figure 10.1 A malicious service agent is unable to retrieve data from an encrypted message. The retrieval attempt may furthermore be revealed to the cloud service consumer. (Note the use of the lock symbol to indicate that a security mechanism has been applied to the message contents.)

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

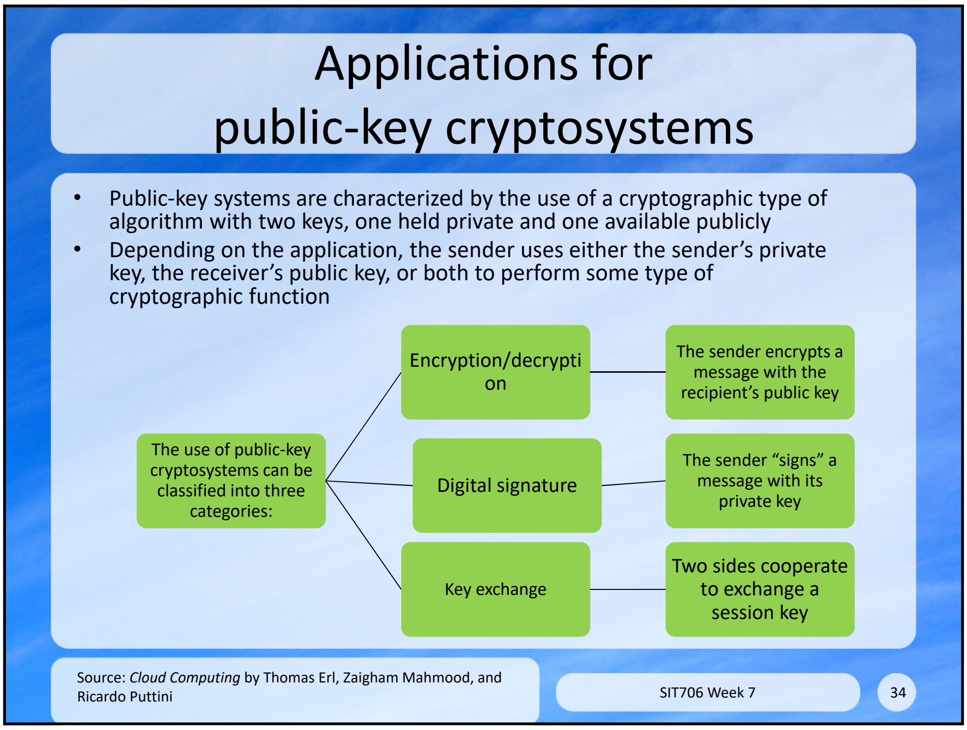
32



Encryption

- Key features of asymmetric encryption:
  - Two keys:
    - Public key: sent to other communicating party/parties
    - Private key: kept secret by one party (the owner)
  - Data encrypted with one key can only be decrypted using the matching key
    - Encrypt with public key, only the owner can decrypt (confidentiality)
    - Encrypt with the private key, anyone with public key can decrypt, but proves the owner sent the message
      - Provides integrity, authenticity and non-repudiation
  - Slower than symmetric encryption

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



Applications for public-key cryptosystems

- Public-key systems are characterized by the use of a cryptographic type of algorithm with two keys, one held private and one available publicly
- Depending on the application, the sender uses either the sender's private key, the receiver's public key, or both to perform some type of cryptographic function

The use of public-key cryptosystems can be classified into three categories:

Encryption/decrypti on

The sender encrypts a message with the recipient's public key

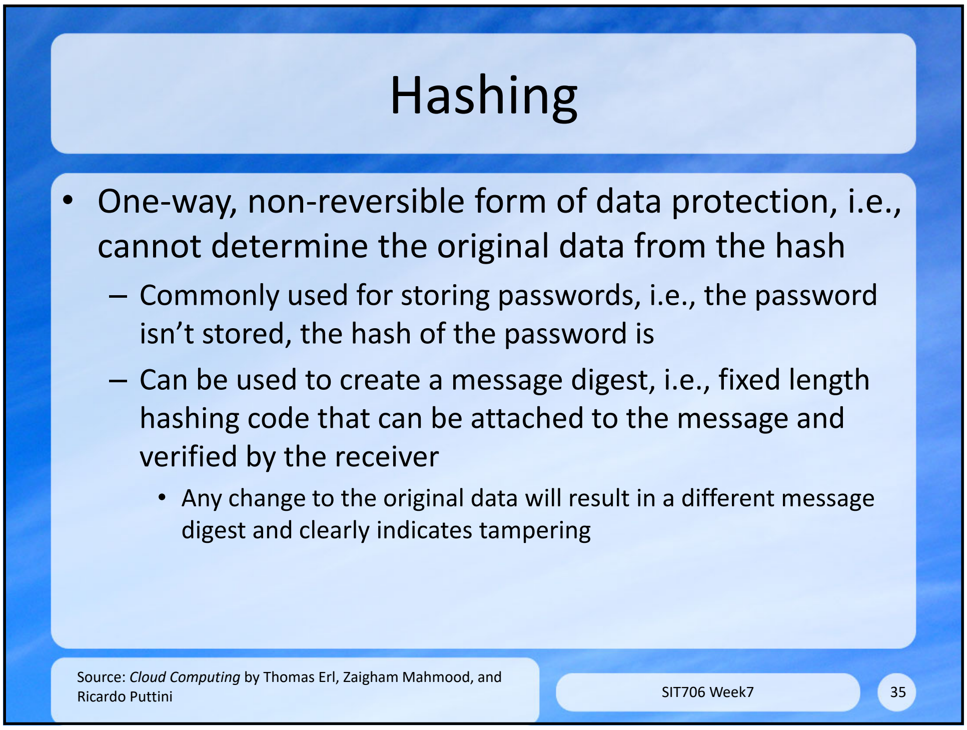
Digital signature

The sender "signs" a message with its private key

Key exchange

Two sides cooperate to exchange a session key

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



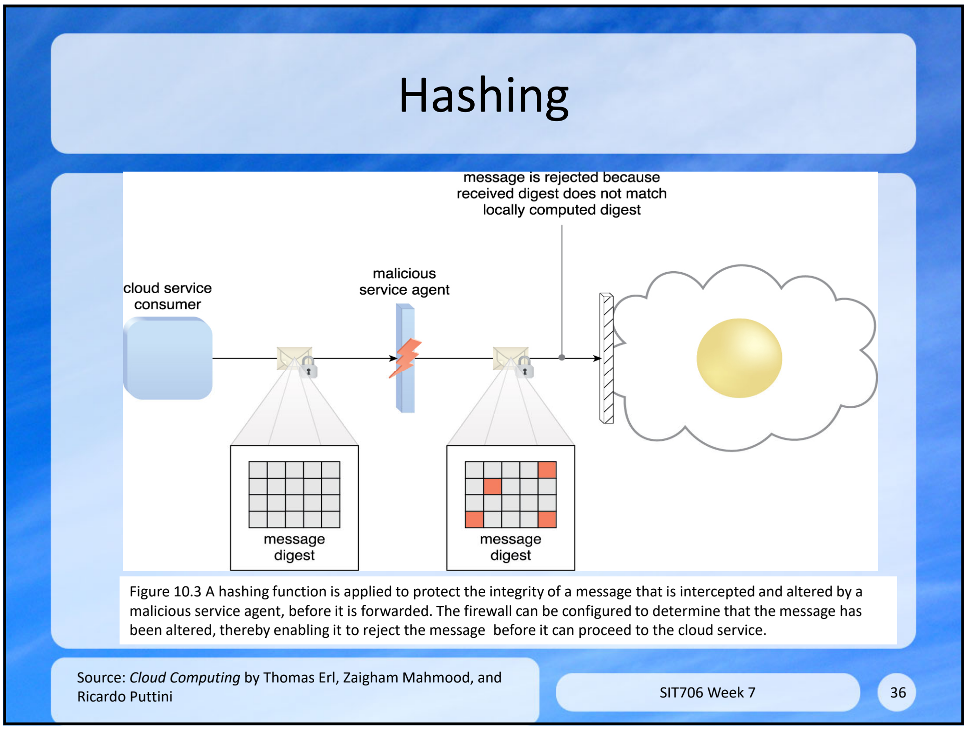
Hashing

- One-way, non-reversible form of data protection, i.e., cannot determine the original data from the hash
  - Commonly used for storing passwords, i.e., the password isn’t stored, the hash of the password is
  - Can be used to create a message digest, i.e., fixed length hashing code that can be attached to the message and verified by the receiver
    - Any change to the original data will result in a different message digest and clearly indicates tampering

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week7

35



Hashing

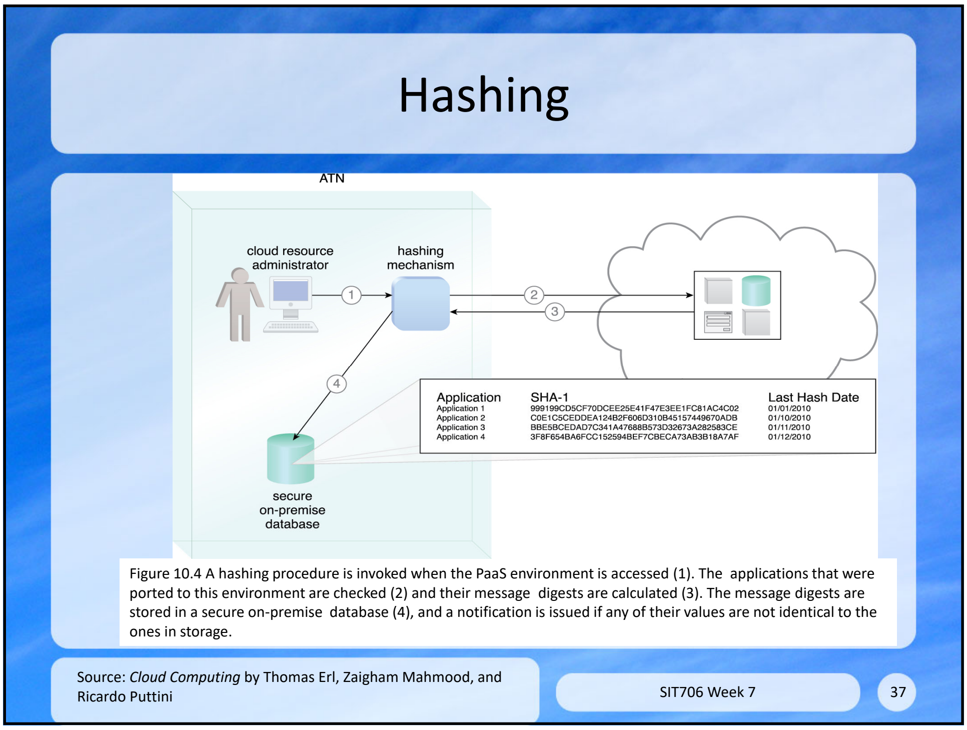
message is rejected because received digest does not match locally computed digest
cloud service consumer
malicious service agent
message digest
message digest

Figure 10.3 A hashing function is applied to protect the integrity of a message that is intercepted and altered by a malicious service agent, before it is forwarded. The firewall can be configured to determine that the message has been altered, thereby enabling it to reject the message before it can proceed to the cloud service.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

36



Hashing

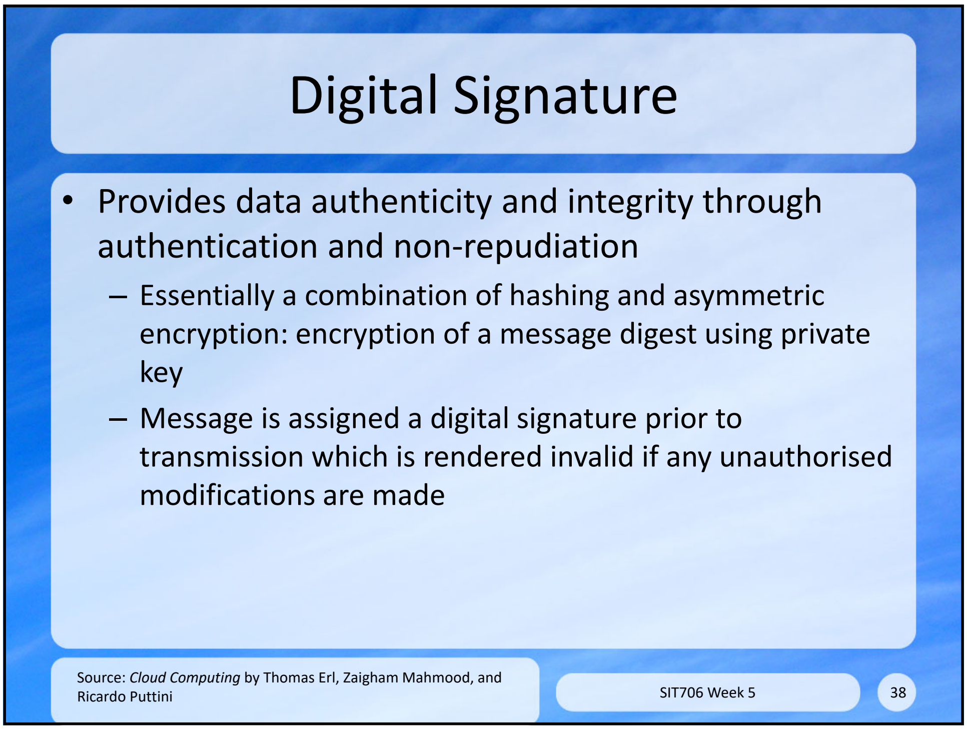
Application	SHA-1	Last Hash Date
Application 1	999199CD5CF70DCEE25E41F47E3EE1FC81AC4C02	01/01/2010
Application 2	C0E1C5CEDDEA124B2F606D310B45157449670ADB	01/10/2010
Application 3	BBE5BCEDAD7C341A47688B573D32673A282583CE	01/11/2010
Application 4	3F8F654BA6FCC152594BEF7CBECA73AB3B18A7AF	01/12/2010

Figure 10.4 A hashing procedure is invoked when the PaaS environment is accessed (1). The applications that were ported to this environment are checked (2) and their message digests are calculated (3). The message digests are stored in a secure on-premise database (4), and a notification is issued if any of their values are not identical to the ones in storage.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

37



Digital Signature

- Provides data authenticity and integrity through authentication and non-repudiation
  - Essentially a combination of hashing and asymmetric encryption: encryption of a message digest using private key
  - Message is assigned a digital signature prior to transmission which is rendered invalid if any unauthorised modifications are made

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 5

38

Digital Signature

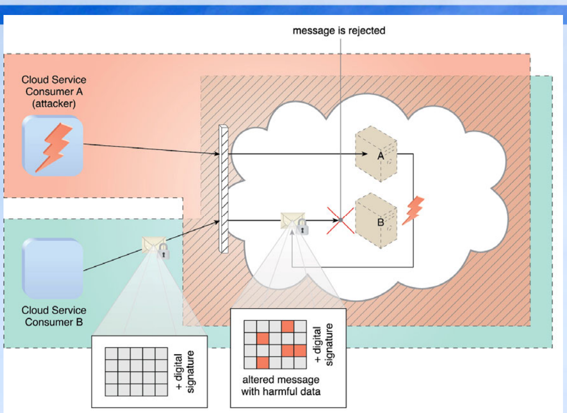


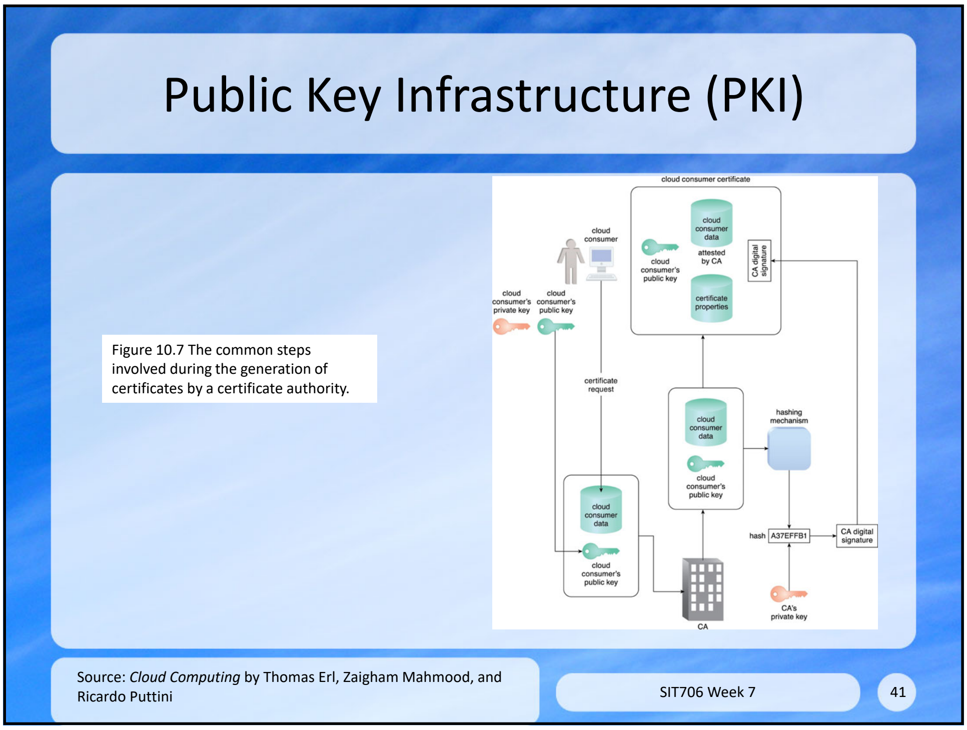
Figure 10.5 Cloud Service Consumer B sends a message that was digitally signed but was altered by trusted attacker Cloud Service Consumer A. Virtual Server B is configured to verify digital signatures before processing incoming messages even if they are within its trust boundary. The message is revealed as illegitimate due to its invalid digital signature, and is therefore rejected by Virtual Server B.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

Public Key Infrastructure (PKI)

- A system of protocols, data formats, rules, and practices for managing the issuance of asymmetric keys
  - Associates public keys with key owners (public key identification) and enables verification of key validity
  - Rely on the use of digital certificates
    - Digitally signed data structures binding public keys to certificate owner identities
    - Usually digitally signed by a third-party certificate authority (CA)
      - Only a handful of trusted CAs, e.g., VeriSign, Comodo

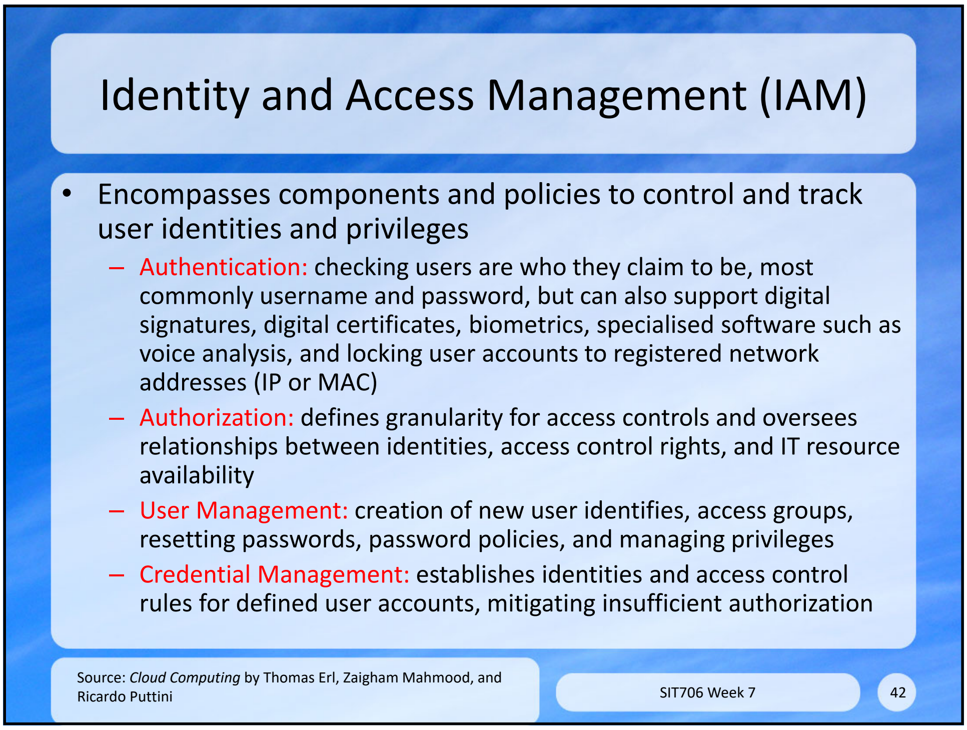
Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



Public Key Infrastructure (PKI)

Figure 10.7 The common steps involved during the generation of certificates by a certificate authority.

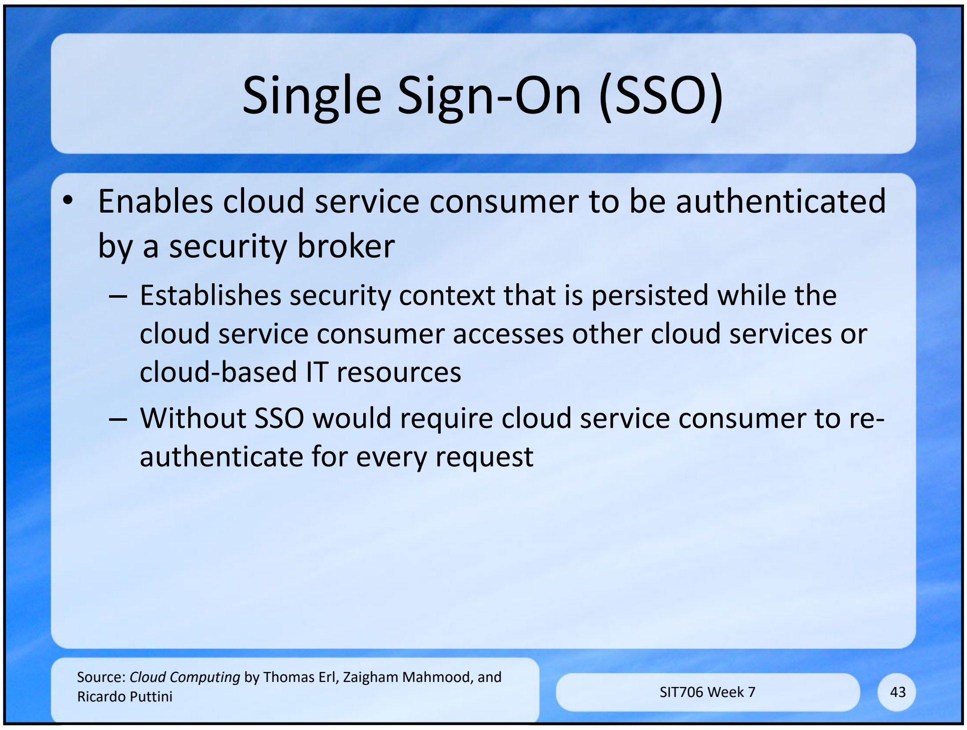
Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



Identity and Access Management (IAM)

- Encompasses components and policies to control and track user identities and privileges
  - Authentication: checking users are who they claim to be, most commonly username and password, but can also support digital signatures, digital certificates, biometrics, specialised software such as voice analysis, and locking user accounts to registered network addresses (IP or MAC)
  - Authorization: defines granularity for access controls and oversees relationships between identities, access control rights, and IT resource availability
  - User Management: creation of new user identifies, access groups, resetting passwords, password policies, and managing privileges
  - Credential Management: establishes identities and access control rules for defined user accounts, mitigating insufficient authorization

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



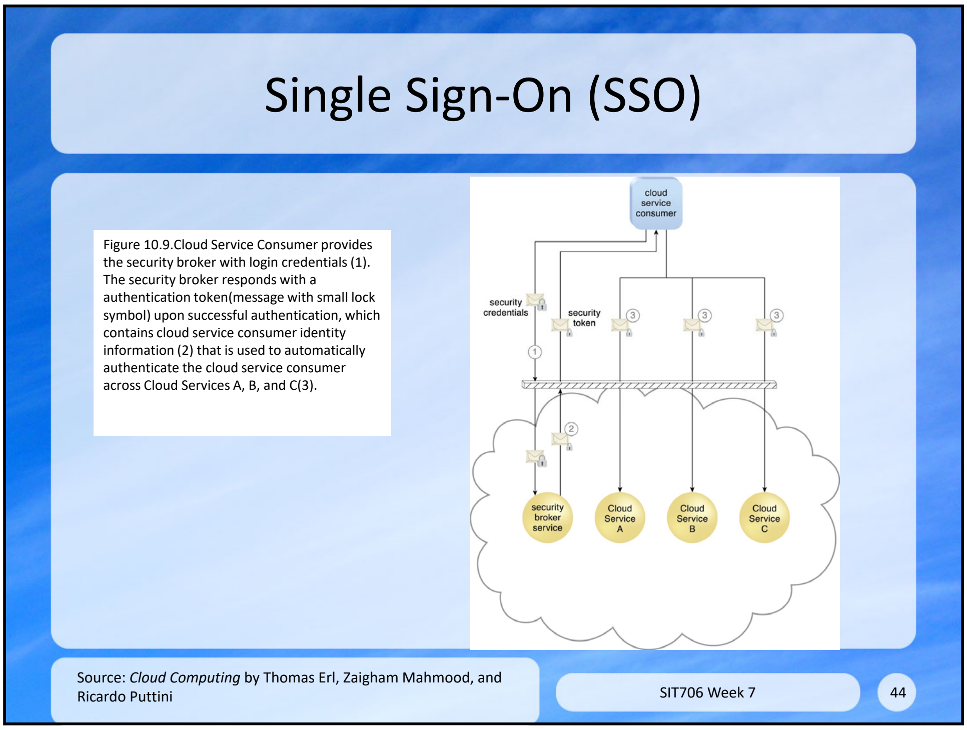
Single Sign-On (SSO)

- Enables cloud service consumer to be authenticated by a security broker
  - Establishes security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources
  - Without SSO would require cloud service consumer to re-authenticate for every request

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

43



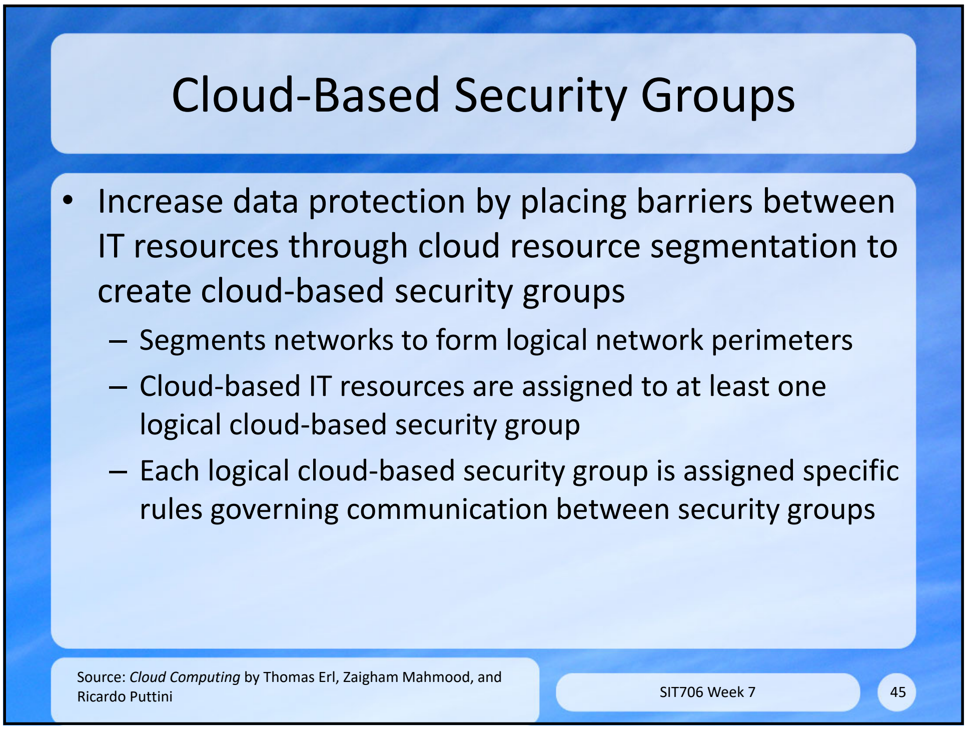
Single Sign-On (SSO)

Figure 10.9.Cloud Service Consumer provides the security broker with login credentials (1). The security broker responds with a authentication token(message with small lock symbol) upon successful authentication, which contains cloud service consumer identity information (2) that is used to automatically authenticate the cloud service consumer across Cloud Services A, B, and C(3).

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

44



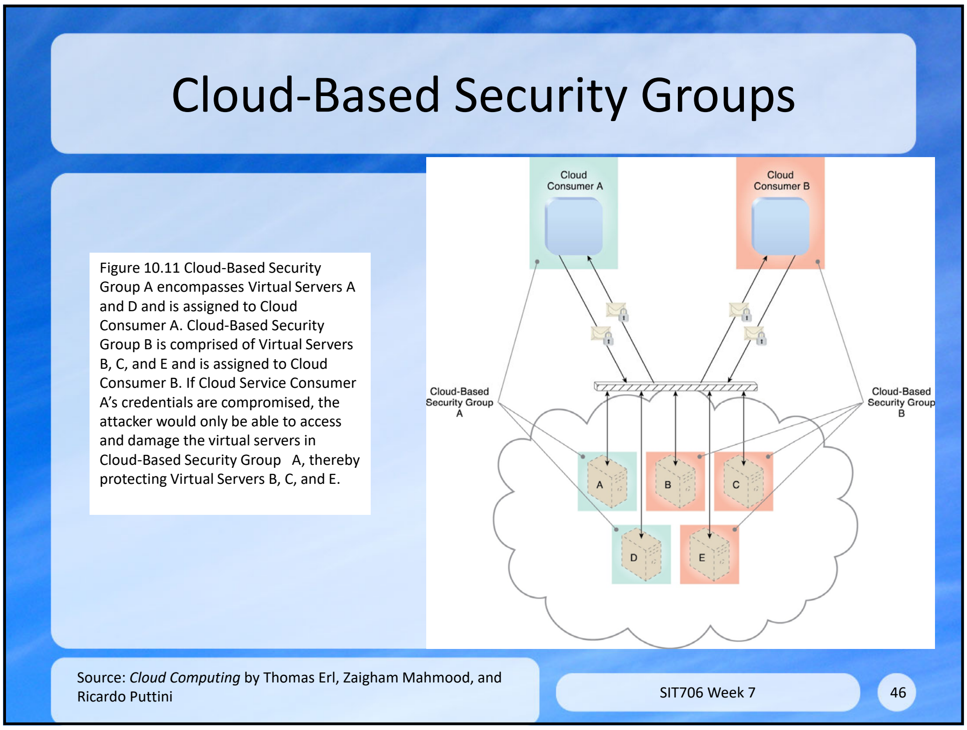
Cloud-Based Security Groups

- Increase data protection by placing barriers between IT resources through cloud resource segmentation to create cloud-based security groups
  - Segments networks to form logical network perimeters
  - Cloud-based IT resources are assigned to at least one logical cloud-based security group
  - Each logical cloud-based security group is assigned specific rules governing communication between security groups

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

45



Cloud-Based Security Groups

Figure 10.11 Cloud-Based Security Group A encompasses Virtual Servers A and D and is assigned to Cloud Consumer A. Cloud-Based Security Group B is comprised of Virtual Servers B, C, and E and is assigned to Cloud Consumer B. If Cloud Service Consumer A's credentials are compromised, the attacker would only be able to access and damage the virtual servers in Cloud-Based Security Group A, thereby protecting Virtual Servers B, C, and E.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

SIT706 Week 7

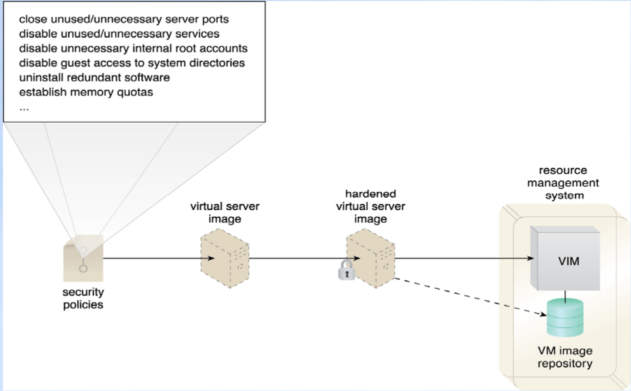
46

Hardened Virtual Server Images

- Stripping of unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers
  - Remove redundant programs
  - Close unnecessary server ports
  - Disable
    - Unused services
    - Internal root accounts (privileged/administrator accounts)
    - Guest access

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

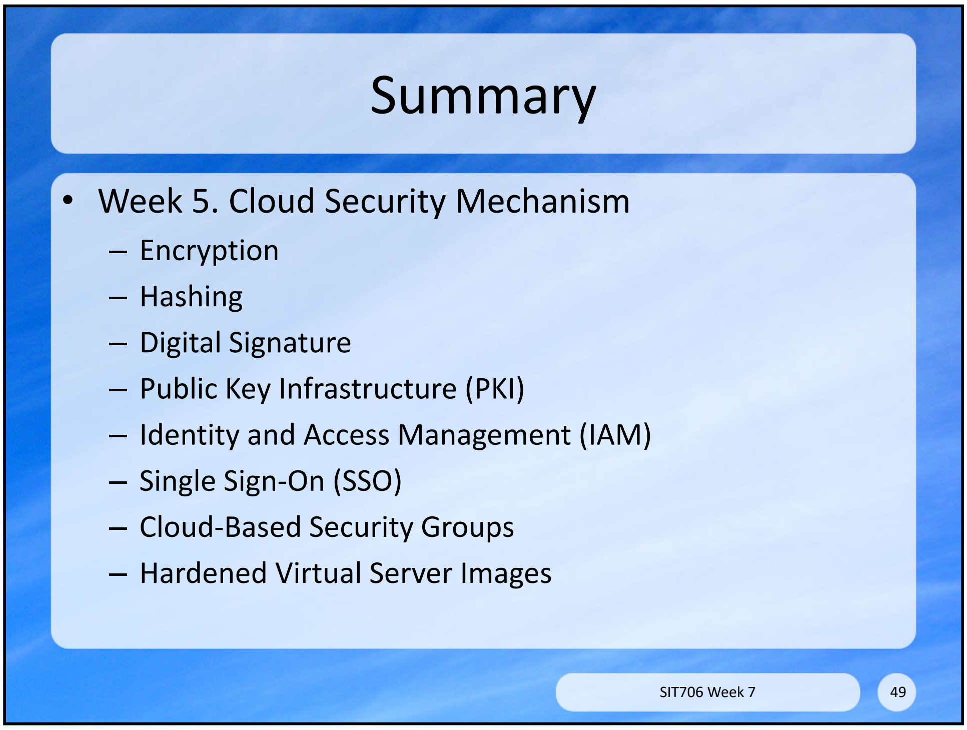
Hardened Virtual Server Images



close unused/unnecessary server ports
disable unused/unnecessary services
disable unnecessary internal root accounts
disable guest access to system directories
uninstall redundant software
establish memory quotas
...

Figure 10.13 A cloud provider applies its security policies to harden its standard virtual server images. The hardened image template is saved in the VM images repository as part of a resource management system.

Source: *Cloud Computing* by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini



Summary

- Week 5. Cloud Security Mechanism
  - Encryption
  - Hashing
  - Digital Signature
  - Public Key Infrastructure (PKI)
  - Identity and Access Management (IAM)
  - Single Sign-On (SSO)
  - Cloud-Based Security Groups
  - Hardened Virtual Server Images