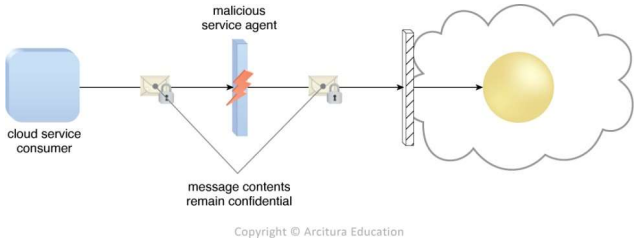
第10章 云安全机制

安全属性

- 保密性(confidentiality)是指只有被授权方才能访问的特性
- 完整性(integrity)是指未被未授权方篡改的特性
- 真实性(authenticity)是指事务是由经过授权的源提供的这一特性
- 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



- *Figure 10.1 - A malicious intermediary 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.)*

加密

- 加密(encryption)
  - 是一种数字编码系统，专门用来保护数据的保密性和完整性。
  - 用于对抗流量窃听、恶意媒介、授权不足和信任边界重叠这样一些安全威胁。
- 加密部件(cipher)
  - 加密用的标准化算法，把原始的明文数据（Plaintext）转换成加密的密文数据（ciphertext）。
- Key – 密钥

加密的类型

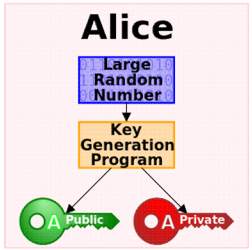
- Stream-based Ciphers
  - One at a time, please
  - Mixes plaintext with key stream
  - Good for real-time services
- Block Ciphers
  - Amusement Park Ride
  - Substitution and transposition

加密的方法

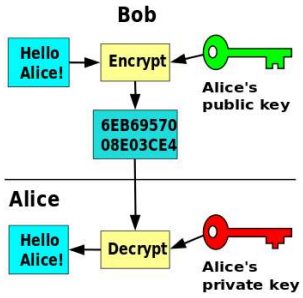
- **Symmetric 对称加密**
  - Same key for encryption and decryption
  - Key distribution problem
- **Asymmetric 非对称加密**
  - Mathematically related key pairs for encryption and decryption
  - Public and private keys
- **Hybrid**
  - Combines strengths of both methods
  - Asymmetric distributes symmetric key
    - Also known as a ***session key***
  - Symmetric provides bulk encryption
  - Example:
    - SSL negotiates a hybrid method

非对称加密

- 基于无法逆向求解的数学问题
  - 整数分解、离散对数、椭圆曲线等。
- 通过一个大的随机数产生一对密钥
  - 私钥、公钥



公钥加密



对称vs.非对称

- 对称加密保证了数据的保密性(confidentiality)但是并不保证数据的不可否认性(non-repudiation)
- 非对称加密依赖于使用两个不用的密钥，称为私钥和公钥。
  - 用自己的私钥加密给对方，对方用公钥解开
    - 真实性、不可否认性和完整性保护（不提供保密性）
  - 用公钥加密送给私钥拥有者
    - 保证了保密性（不保证完整性、真实性的保护）

Symmetric Algorithms

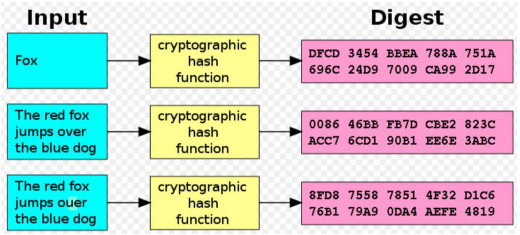
- DES
  - Modes: ECB, CBC, CFB, OFB, CM
- 3DES
- AES
- IDEA
- Blowfish
- RC4
- RC5
- CAST
- SAFER
- Twofish

Asymmetric Algorithms

- Diffie-Hellman
- RSA
- El Gamal
- Elliptic Curve Cryptography (ECC)

§ 10.2 哈希 Hashing

- 哈希(Hashing)
  - 用来获得消息的哈希代码或消息摘要(message digest)，通常是固定的长度，小于原始的消息大小。
  - 单向的、不可逆转的数据保护。



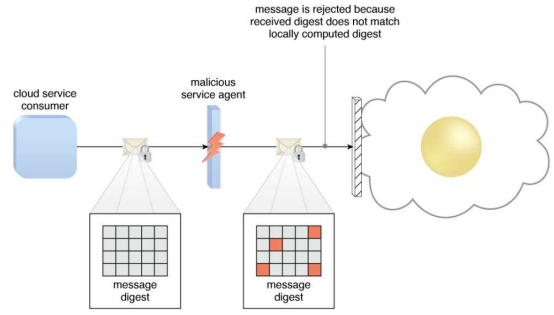
哈希算法

哈希函数的主要属性：
计算简单、不可逆、不重复

- MD5
  - Computes 128-bit hash value
  - Widely used for file integrity checking
- SHA-1（新版本为SHA-2）
  - Computes 160-bit hash value
  - NIST approved message digest algorithm
- HAVAL
  - Computes between 128 and 256 bit hash
  - Between 3 and 5 rounds
- RIPEMD-160
  - Developed in Europe published in 1996
  - Patent-free

哈希的典型应用

- 数据保密
  - 如密码哈希（Password verification）
- 恶意媒介和授权不足
  - Verifying the integrity of files or messages
- 服务滥用（如DoS）
  - Proof-of-work，要求服务请求者产生能生成特种Hash值的消息
- 文件标识
  - P2P文件系统、软件版本管理工具等
- 3.5 Pseudorandom generation and key derivation



- *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.*

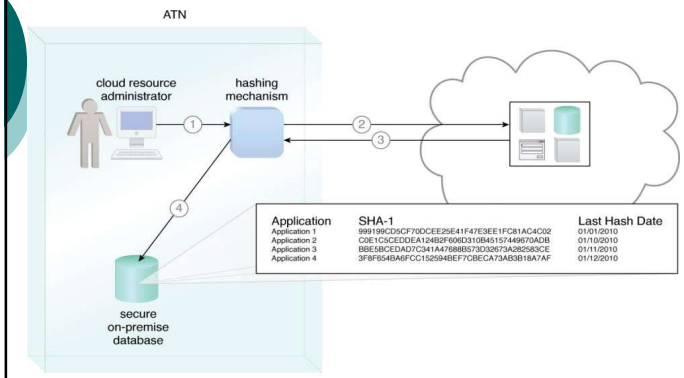
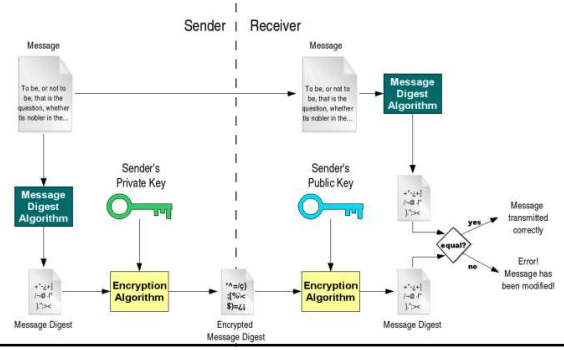


图 10.4哈希摘要用于保障应用程序的完整性。

§ 10.3 数字签名

- 数字签名(digital signature)
  - 将消息进行哈希，然后用私钥进行加密。



数字签名

- 作用：
  - 提供不可否认性、数据真实性和数据完整性。
  - 类似于日常生活中的“签名”。
- 算法：
  - RSA是最常用的签名算法。
- 扩展应用：
  - 数字证书：个人安全邮件证书
  - 智能卡：将数字签名放入便携物理存储介质

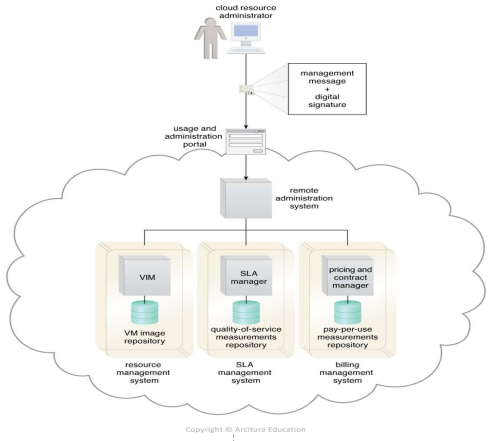
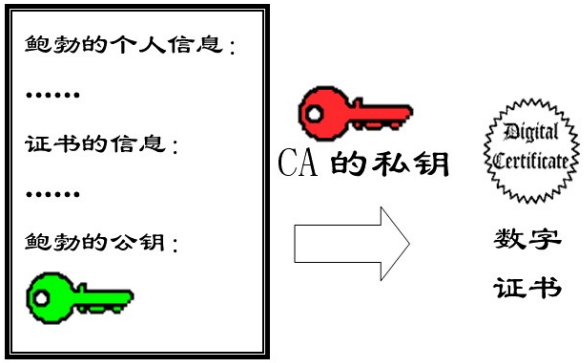


图 10.6 基于数字签名的云管理保障

§ 10.4 公钥基础设施

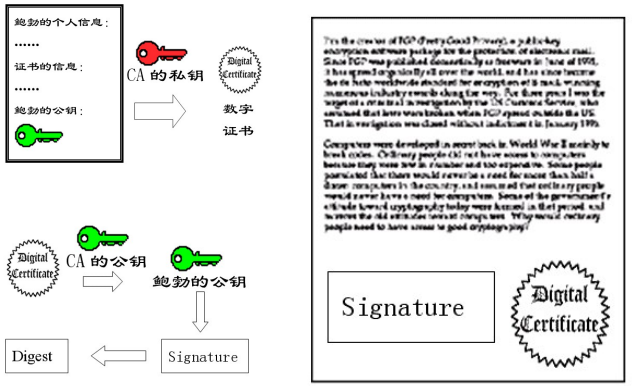
- 公钥基础设施(The public key infrastructure, PKI)
  - 是一个由协议、数据格式、规则和实施组成的系统
  - 是用于大规模、公共系统的公钥加密技术
- 数字证书：
  - 带数字签名的数据结构，验证证书拥有者身份以及相关信息。
  - 通常是由第三方证书颁发机构(certificate authority) 签发的，比如和VeriSign 和 Comodo

数字证书

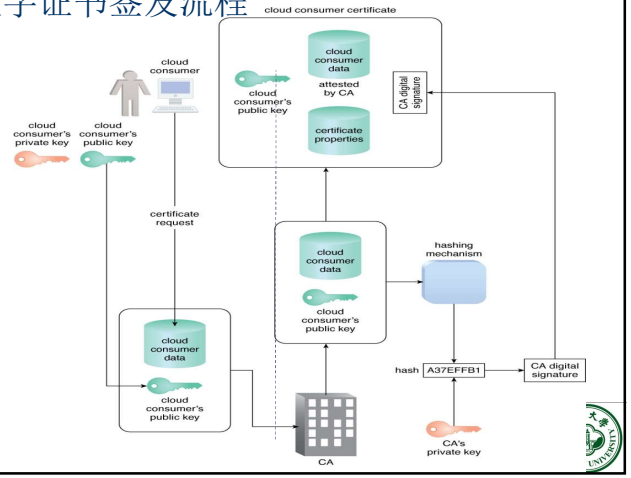


数字证书

证书：安全传送发送者的公钥；
签名：确认数据是发送者发送并且未被篡改。



数字证书签发流程



PKI与云计算

- 实现非对称加密
- 管理云用户和云提供者身份信息
- 防御恶意中介和不充分的授权威胁

§ 10.5 身份与访问管理 IAM

- 身份与访问管理(identity and access management)
  - 控制和追踪用户身份以及
  - IT资源、环境、系统访问特权
- 四部分组成
  - 认证(Authentication)
  - 授权 (Authorization)
  - 用户管理(User Management)
  - 证书管理(Credential Management)

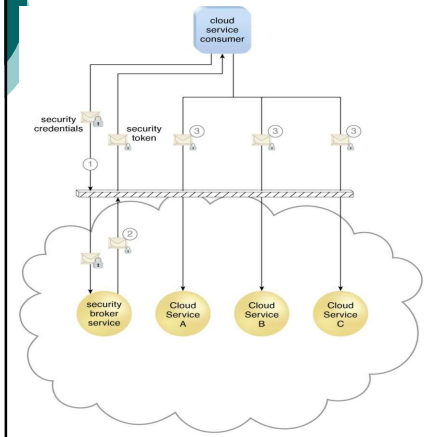
身份与访问管理

- IAM机制功能：
  - 分配用户特权等级
  - 访问控制和策略
- IAM机制的用途：
  - 对抗授权不足、拒绝服务攻击和信任边界重叠等威胁
  - 比PKI机制要更全面

§ 10.6 单一登录

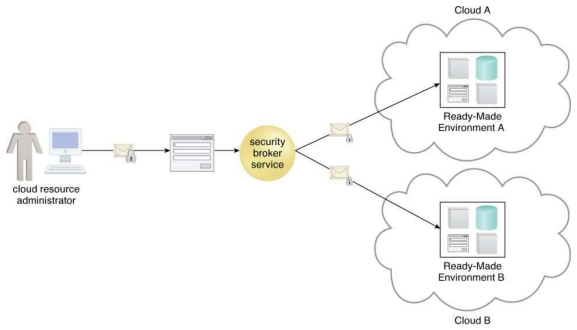
- 单一登录(single sign-on ,SSO)机制
  - 使得一个云服务用户能够被一个安全代理认证并建立起一个安全上下文
  - 当云用户要访问其他云服务或资源的时候，这个上下文会被持久化。
- 实现跨云服务的用户认证和授权

SSO基本示例



- *A cloud service consumer provides the security broker with login credentials (1).*
- *The security broker responds with an 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 for Cloud Services A, B, and C (3).*

图10.10 (ATN's Example)



- *Figure 10.10 - The credentials received by the security broker are propagated to ready-made environments across two different clouds. The security broker is responsible for selecting the appropriate security procedure with which to contact each cloud.*

单一登录

- SSO机制实际上允许互相独立的云服务和IT资源产生并流通运行时认证和授权证书。
- SSO机制实际上并不直接对抗任何一个云安全威。
- SSO增强了基于云的环境的访问并管理分布式IT资源和解决方案的可用性。

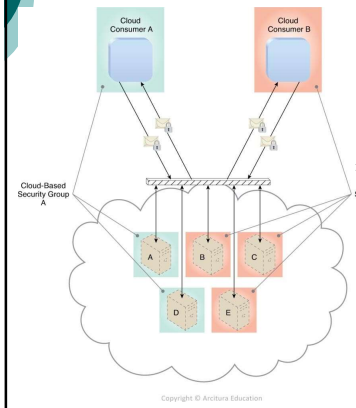
§ 10.7 基于云的安全组

- 云资源分割(segmentation)
  - 为不同用户和组创建各自的物理和虚拟IT环境的过程。
  - 云资源分割是虚拟化的基础
- 基于云的安全组(cloud-based security group)
  - 基于云的资源分割，网络被分成逻辑的基于云的安全组，形成逻辑网络边界。

基于云的安全组

- 运行在同一个物理服务器上的多个虚拟服务器逻辑上可以是不同基于云的安全组的成员。
- 基于云的安全组能限制对资源的未被授权的访问。
- 用来对抗
  - 拒绝服务、授权不足和信任边界重叠等威胁

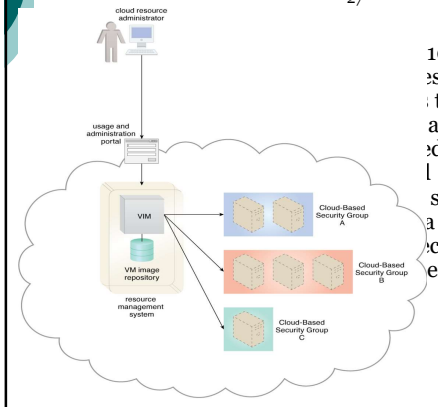
图10.11



•Figure 10.11 - A logical cloud-based security group, Group A, is comprised of Virtual Servers A and D and assigned to Cloud Consumer A, while Group B is comprised of Virtual Servers B, C, and E and assigned to Cloud Consumer B. If Cloud Service Consumer A's user account is compromised, the attacker would only be able to damage the servers in Security Group A, thereby protecting Virtual Servers B, C, and E.

图10.12 (DTGOV's Example)

27

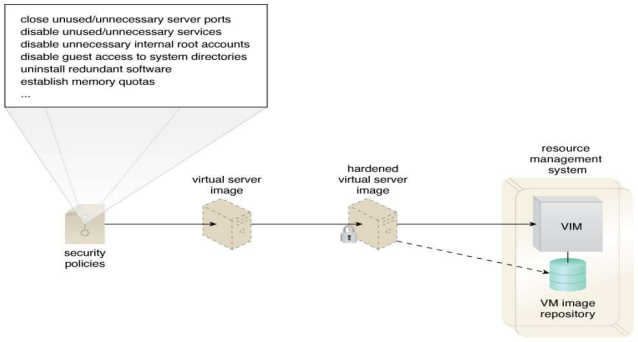


10.12 - When an external esource administrator the Web portal to a virtual server, the d security controls are and mapped to an security policy that a corresponding cloud- curity group to the new erver.

§ 10.8 强化的虚拟服务器映像

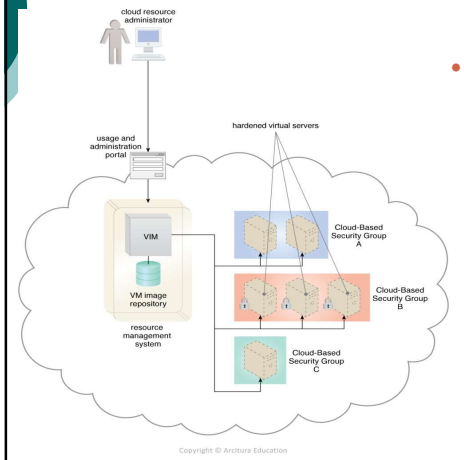
- 虚拟服务器镜像(VM image)
  - 一个从模板配置创建的虚拟服务器镜像
  - 比原始标准映像更加安全的虚拟服务器模板
- 强化(Hardening)
  - 把不必要的软件从系统中剥离出来，限制可能被攻击者利用的潜在漏洞的过程。
  - 去除冗余的程序，关闭不必要的服务器端口，关闭不使用的服务，内部root用户和guest访问等。
- 对抗拒绝服务、授权不足和信任边界重叠等威胁。

图10.13



- *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.*

图10.14 (DTGOV's Example)



- Figure 10.14 - The cloud resource administrator chooses the hardened virtual server image option for the virtual servers provisioned for Cloud-Based Security Group B.

本章小结

- 云安全的基本措施和技术
  - 加密、哈希、签名、PKI
- 云安全的相关机制
  - 身份认证与访问控制
  - 单一登录
  - 安全组
  - 虚拟服务器强化

课后题

无。