Tecnologías Grid

Seguridad en entornos grid

Master en Sistemas y Servicios Informáticos para Internet
Área de Arquitectura y Tecnología de Computadores
Universidad de Oviedo

Seguridad en entornos grid

Introducción

Introducción

- Objetivos
  - Coordinar la seguridad en organizaciones virtuales (VO)
  - Necesidades básicas
    - Autenticación
    - Autorización
    - Delegación
  - Aspectos convenientes
    - Confidencialidad de mensajes
    - No repudio
    - Integridad de los mensajes

Introducción

- Fundamentos de criptografía

USOS	SERVICIO	PROTEGE CONTRA
Mantener el secreto	Confidencialidad	Escucha a escondidas
Probar la identidad	Autenticación	Falsificación y suplantación
Verificar la información	Integridad	Alteración

- Ejemplo (I)
  - A envía una postal a B y C trata de actuar sobre la postal
    - ¿Cómo garantizar qué sólo B pueda leer la postal?
    - ¿Cómo garantizar que fue A quien envió la postal?
    - ¿Cómo sabe B que la postal no ha sido alterada?

Introducción

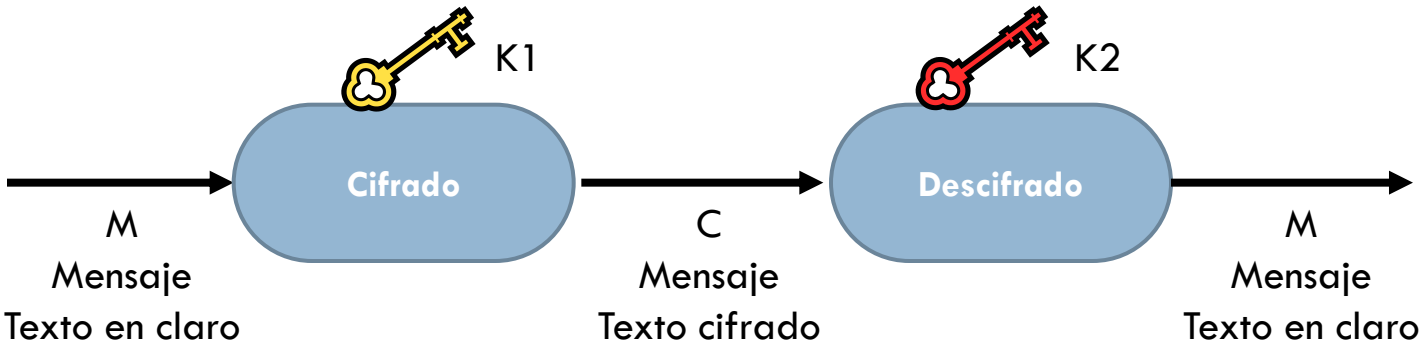
- Ejemplo (II)
  - Mantener el secreto
    - A cifra el texto y B lo descifra
    - A y B deben compartir un sistema de cifrado que C desconozca
  - Probar la identidad
    - A incluye una frase secreta que sólo B conoce
  - Prevenir alteraciones
    - A calcula un valor a partir de la información de la postal, le suma un valor sólo conocido por B y lo incluye en la postal

Seguridad en entornos grid

Cifrado

Cifrado

- Base
  - Algoritmos de cifrado y descifrado



  - Tipos de algoritmos
    - Simétricos o de clave secreta: K1 = K2
    - Asimétricos o de clave pública: K1 ≠ K2

Cifrado

- Algoritmos simétricos
  - A y B utilizan la misma clave
    - Y el resto del mundo debe desconocerla
  - Efectividad del cifrado función de la longitud de la clave
  - Desventajas
    - ¿Cómo intercambian A y B la clave sin que nadie se entere?
    - Número de claves $O(n^2)$ con n = número de usuarios
  - Algoritmos más comunes
    - DES, 3DES, AES, RC2, RC4

Cifrado

- Algoritmos asimétricos (I)
  - A y B utilizan dos claves distintas
    - Lo que una clave cifra, la otra lo descifra y viceversa
  - Proceso
    - B crea dos claves
      - Pública: la puede conocer todo el mundo
      - Privada o secreta: sólo la conoce B
    - B difunde su clave pública, que lee A
    - A cifra el mensaje con la clave pública de B
    - A envía el mensaje a B
    - B lo descifra con su clave privada
  - Algoritmo asimétrico más habitual: RSA

Cifrado

- Algoritmos asimétricos (II)
  - Consideraciones
    - A no podría descifrar su propio mensaje
      - No conoce la clave privada de B
    - Si B quiere enviar algo a A, necesita la clave pública de A
      - Tiene que haber cuatro claves para una comunicación bidireccional
    - El coste computacional de cifrado de clave pública es alto
      - Solución: combinación de algoritmos simétricos y asimétricos

Cifrado

- Combinación de algoritmos
  - Usada en TLS/SSL
  - Pasos
    - B crea dos claves (pública y privada) y difunde la pública
    - A lee la clave pública de B, genera una lista de números aleatorios, la cifra con la clave pública de B y se la envía
    - B descifra la lista con su clave privada
      - Sólo él puede hacerlo
    - A y B usan la lista de números aleatorios como clave secreta
      - El resto de comunicaciones utilizan clave secreta

Cifrado

- Aplicaciones
  - Aplicación 1:
    - B prueba su identidad a A
      - B cifra una información X (conocida por A y B) con la clave privada de B
      - B envía la información a A
      - A descifra la información con la clave pública de B
        - Si coincide con X, tuvo que haberla enviado B
  - Aplicación 2
    - Firmas digitales
      - A cifra una información con su clave privada
      - Cualquiera puede descifrarla con la clave pública de A...
      - ...sabiendo que sólo A ha podido ser el autor

Cifrado

- Firmas digitales (I)
  - Demuestran la autenticidad de una información
    - A quiere asegurar que un mensaje es suyo
    - A calcula un hash E del mensaje
      - Para tener que cifrar menos información
    - A cifra con su clave privada el hash → «firma digital»
    - B lee el mensaje y la firma digital
    - Calcula un hash R del mensaje recibido
    - Descifra con la clave pública de A la firma digital
      - Obtiene el hash E
    - Si R = E, B se asegura de que
      - El mensaje fue generado por A
      - Nadie modificó el mensaje

Cifrado

- Firmas digitales (II)
  - Funciones hash
    - Para que todo funcione, hay que utilizar funciones hash criptográficas
    - Función hash H
      - A partir de una información M de longitud variable produce una cadena H(M) = h de longitud fija
    - Funciones hash criptográficas
      - Dado M, debe ser fácil calcular h
      - Dado h, debe ser difícil calcular M
      - Debe ser difícil calcular M' tal que H(M') = h
    - Más habituales: MD4, MD5, SHA

Seguridad en entornos grid

Aplicación a grid

Certificados digitales

- Para que la firma digital sea útil
  - La clave privada de A sólo debe ser conocida por A
  - B debe tener acceso a la clave pública de A
  - B debe estar seguro de que la clave pública es realmente de A
    - ¿Quién asegura esto?
- Autoridad de certificación (CA)
  - Entidad que certifica que una clave pública se corresponde con un propietario
  - Las autoridades de certificación se integran en una infraestructura de clave pública (PKI)

Certificados digitales

- Infraestructura de clave pública (I)
  - Conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, distribuir, almacenar y revocar certificados digitales
    - Necesario cuando dos personas no pueden intercambiar sus claves con confianza
  - El estándar X.509 especifica
    - Formatos de certificados de clave pública, listas de revocación de certificados y certificados de autorizaciones
    - Algoritmo de para validar cadenas de certificados
      - Las CA están organizadas en una estructura jerárquica

Certificados digitales

- Certificado digital
  - Asocian un nombre con una clave pública
  - Son firmados por el emisor
  - Información básica que contienen
    - Emisor (CA)
    - Período de validez
    - Nombre del usuario
    - Clave pública del usuario
    - Firma del certificado

Certificados digitales

```
Certificate:
Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e95)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
            OU=Certification Services Division,
            CN=Thawte Server CA/emailAddress=server-certs@thawte.com
    Validity
        Not Before: Jul  9 16:04:02 1998 GMT
        Not After : Jul  9 16:04:02 1999 GMT
    Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
             OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                e8:35:1c:9e:27:52:7e:41:8f
            Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
    93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
    92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
    ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
    d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
    0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
    5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
    8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
    68:9f
```

Autoridad Certificadora

Usuario

Clave pública del usuario

Firma digital del certificado por la autoridad certificadora

Certificados digitales

- Solicitud de certificados
  1. El usuario genera las claves
     - Clave privada: la guarda en disco
     - Clave pública: la añade a una solicitud de certificado y la envía a la CA
  2. La CA le envía al usuario un código de solicitud
  3. El usuario lleva el código de solicitud y un documento de identificación a una oficina de registro
  4. La oficina valida la identidad del usuario y lo comunica a la CA
  5. La CA crea, firma y emite el certificado del usuario

Certificados digitales

- En entornos grid
  - Cada usuario, host o servicio tiene un certificado X.509
  - Los certificados están firmados por las CA locales
  - Cada transacción en grid requiere autenticación mutua
    - A envía su certificado
    - B verifica la firma en el certificado de A usando el certificado de la CA
    - B envía a A una cadena de prueba
    - A cifra la cadena con su clave privada y la envía a B
    - B usa la clave pública de A para comprobar la identidad de A