VNIVERSITAT DE VALÈNCIA

Seguridad

MASSDE

Seguridad

Elementos de seguridad en…

- Seguridad en las comunicaciones:
  - Prevenir la comprensión de las comunicaciones intervenidas (Secreto).
  - Establecer la identidad del remitente de una comunicación (Autentificación).
  - Establecer que una comunicación no ha sufrido ningún tipo de intromisión (Integridad).

3

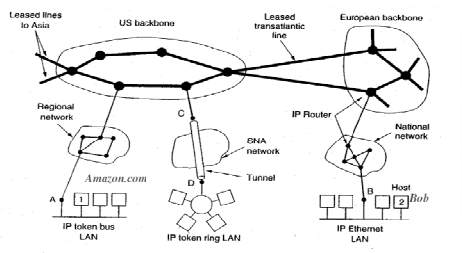
Elementos de seguridad en…

- Seguridad en el acceso a recursos:
  - Establecer identidad del solicitante (Autentificación).
  - Permitir o denegar el acceso (Autorizar).

4

¿Comunicaciones seguras?

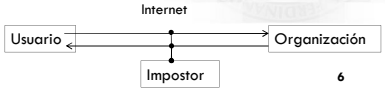
- ¿Qué puede ir mal?



5

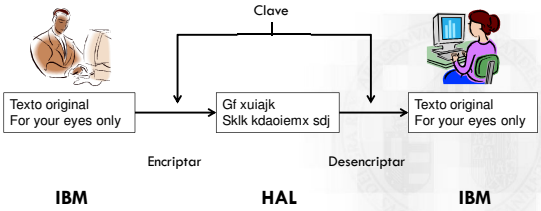
Seguridad en la comunicación

- Encriptación:
  - ¿Cómo asegurar que las transacciones son secretas?
- Autentificación:
  - ¿Cómo verificar la identidad **real** de mis interlocutores?
- Integridad:
  - ¿Cómo asegurar que el mensaje no ha sido alterado?



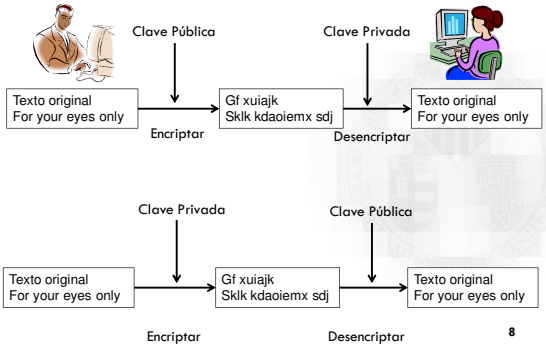
6

Criptografía tradicional (de clave secreta)



7

Criptografía de clave pública



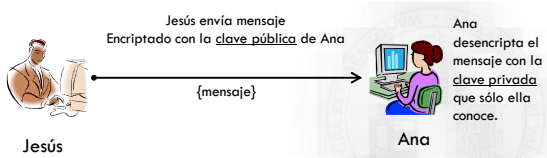
8

Criptografía de clave pública (2)

- Criptografía de clave secreta:
  - La misma clave secreta se utiliza para encriptar y para desencriptar.
  - Problema: ¿Cómo transmitir la clave de manera segura por internet?
- Criptografía de clave pública:
  - Clave pública conocida por todo el mundo para encriptar (se puede transmitir sin problemas).
  - Clave privada conocida sólo por el propietario para desencriptar (no hace falta transmitirla).

9

Criptografía de clave pública (3)



10

La clave pública funciona si…

- La clave privada permanece secreta:
  - Nunca abandona el ordenador del propietario.
  - Normalmente encriptada y protegida con clave.
- Dificultad de adivinar la clave privada conociendo la clave pública:
  - Necesidad de probar todas las combinaciones posibles.
  - La dificulta de "romper" el código se incrementa exponencialmente con la longitud de la clave.
  - Claves de 1024 bits requieren más tiempo que la edad del universo para "romperse".

11

Encriptar no es suficiente

- Hacerse pasar por otro (suplantar identidad)
- Es difícil conectarse a una máquina sin la palabra clave pero es fácil enviar información con el nombre de otra persona (email).

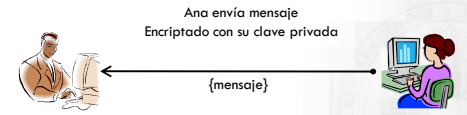
12

Firma digital

- La clave pública y la clave privada se pueden aplicar en cualquier orden.
- Ana tiene que enviar un mensaje M a Jesús
  - Aplica su clave privada
  - Envía el mensaje encriptado a Jesús
- Jesús desencripta el mensaje con la clave pública de Ana
  - Recupera el mensaje original.
  - Infiere que Ana es el remitente original, puesto que sólo Ana conoce la clave privada que se corresponde con su clave pública.
- Encriptar el mensaje con la clave privada actúa como firma digital.

13

Firma digital (2)



Jesús desencripta el mensaje con la clave pública de Ana y está "seguro" de que Ana es la remitente.

14

Gestión de la clave pública

- ¿Dónde se almacenan las claves públicas?
  - Servidores de claves públicas. Ejemplo:
    - *http://www.rediris.es/keyserver/*

15

Posible problema

- Falsificación de la clave pública
- El sistema solo funciona si la clave pública se obtiene de una fuente de confianza

16

Certificados

- Utilizados para certificar la identidad de un usuario frente a otro.
  - Nombre del emisor del certificado.
  - A quien certifica
  - La clave pública
- Los certificados están firmados digitalmente por un emisor.
- El emisor debe de ser una entidad de confianza.
- Todos los usuarios deben tener la clave pública del emisor para verificar la firma del certificado.

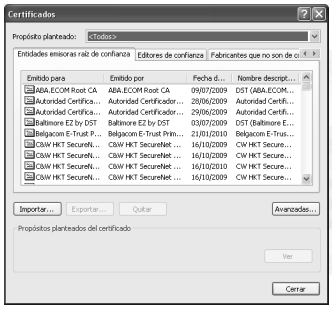
17

Autoridades Certificadoras

- Las Autoridades Certificadoras son entidades con la responsabilidad de generar certificados fiables a los individuos que los soliciten.
  - Los certificados incluyen la clave pública y están firmados por AC.
  - La AC verifica la identidad del solicitante antes emitir el certificado.

18

Certificados en los navegadores



19

Aplicaciones: Comercio Electrónico

- eCommmerce: Necesidad de transmitir información "sensible" a través de la web:
  - Números de tarjetas de crédito
  - Ordenes de compra
- Requisitos:
  - Cliente y servidor (emisor y receptor) deben autentificarse antes de enviar datos.
  - Los datos deben transmitirse firmados

20

HTTPS

- El protocolo HTTPS es la versión segura del protocolo HTTP.
  - Crea un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP.
- Para que un servidor web acepte conexiones HTTPS el administrador debe crear un certificado para el servidor.

21

Seguridad de Acceso a recursos

- Control de acceso:
  - Usuarios autorizados con clave personal
  - Sistemas biométricos
  - Tarjetas inteligentes

22

Usuarios autorizados con clave

- Procedimiento de acceso al recurso (ordenador, página web, etc) basado en una clave personal.
- Debilidades del procedimiento:
  - Palabras claves sencillas o "adivinables"
  - Conocimiento de la clave por terceras personas:
    - De manera involuntaria
    - Comunicaciones interceptadas

23

Sistemas biométricos

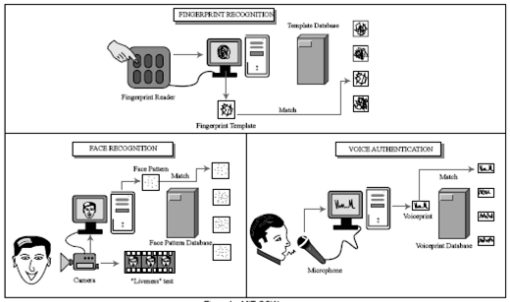


Figure by MIT OCW.

24

Tarjetas inteligentes

- Diversas categorías y tecnologías.
- Tarjetas criptográficas:
  - Almacenan el certificado digital del usuario y su clave privada.
  - La clave privada no reside en el ordenador y, por tanto, no se puede obtener fraudulentamente de él.
  - Emitidas por entidades certificadoras.
  - Son precisos lectores de tarjetas.
- DNI electrónico.

25

Las puertas traseras

- Se trata de "agujeros" (fallos) en aplicaciones del sistema que permiten saltar el control de acceso:
  - Virus
  - Ataques por desbordamiento de memoria
  - …

26

Virus, gusanos (*worms*) y troyanos

- Son programas que se ejecutan en el ordenador sin el conocimiento y/o el consentimiento del propietario/adminitrador y cuyo objetivo suele ser causar algún tipo de perjuicio a los usuarios.
- Se transmiten a través de los canales de E/S.
- Para evitar que entren en nuestro ordenador y/o eliminarlos:
  - Antivirus
  - Firewall

27

Spyware, Adware

- Programas incorporados a nuestro ordenador sin nuestro conocimiento y que hacen cosas no deseadas como:
  - Abrir contenidos no deseados en *pop-ups*
  - Enviar información sobre el ordenador o sus usuarios a otros sistemas.
- Se transmiten a través de:
  - Páginas web
  - Otros programas

28

Ataque por denegación de servicio

- Inundar de peticiones de acceso a la máquina utilizando direcciones IP falsas.
- El ataque se suele producir desde diversas máquinas donde el generador del ataque ha entrado fraudulentamente.
- Ejemplos:
  - eBay
  - Yahoo
  - Amazon

29

Medidas de defensa

- Antivirus
- Firewall
- Sistemas de detección de intrusos

30

¿Qué hace un Firewall?

- Revisa los paquetes que entran y salen de la red y acepta o rechaza en función de las reglas definidas por el usuario.
- Reconoce y bloquea paquetes correspondientes a ataques típicos.

31

Otras medidas preventivas

- Los IDS (sistemas de detección de intrusos) utilizan técnicas de minería de datos para descubrir e informar sobre actividades sospechosas.
- Conviene estar al día en la instalación de "parches" del sistema operativo que tengamos instalado.

32

A pesar de todas las prevenciones…

- Los incidentes de seguridad siguen creciendo.
- Cada vez hacen falta menos conocimientos técnicos para generar ataques sofisticados:
  - Herramientas
  - Información pública

33