Seguridad en Redes

Introducción

Múltiples aspectos de seguridad en redes

- **Confidencialidad**: Solo accede a la información quien debe hacerlo (entidades autorizadas). Aunque haya terceros en el canal los mensajes son solo comprensibles para los interesados.
- **Autenticación**: Las entidades son quien dicen ser (garantiza que A es realmente la persona A y no otra suplantando su identidad).
- **Control de accesos**: Los servicios están accesibles sólo para entidades autorizadas (Ej. A un correo electrónico solo debe acceder su dueño).
- **No repudio**: El sistema impide la renuncia de la autoría de una determinada acción (no se puede negar se el autor de una acción realizada).
- **Integridad**: El sistema detecta todas las alteraciones (intencionadas o no) de la información.
- **Disponibilidad**: Mantener las prestaciones de los servicios con independencia de la demanda (independientemente del nº de usuarios (1, 1 millón o más) el sistema debe seguir prestando sus servicios).

Una red de comunicaciones es **segura** cuando se garantizan todos los aspectos.
No hay protocolos ni redes 100% seguros.
La seguridad de un sistema se debe situar en todos sus niveles/capas. El grado de seguridad lo determina el punto más débil.
Ataque de seguridad: cualquier acción intencionada o no que menoscaba cualquiera de los aspectos de la seguridad.
Tipos de Ataques:

- **Sniffing** → vulneración a la confidencialidad, escuchas (husmear).
- **Spoofing (phising)** → Suplantación de la identidad de entidades
- **Man_in_the_middle** → interceptar tráfico entre dos entidades haciendo spoofing.
- **DDoS** (Distributed Denial_of_Service) → denegación de servicio distribuido, ejemplo **Flooding** (inundación).
- **Malware** → troyanos, gusanos, spyware, backdoors, rootkits, ransomware, keyloggers.

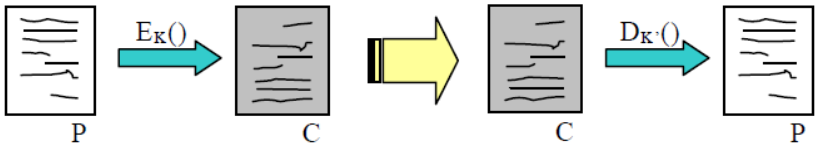
Mecanismos de Seguridad

- **De Prevención**:
  - Mecanismos de autenticación e identificación.
  - Mecanismos de control de acceso.
  - Mecanismos de separación (física, temporal, lógica, …).
  - Mecanismos de seguridad en las comunicaciones (cifrado de información).
- **De detección**:
  - IDS (Intruder Detection System)
- **De recuperación**:
  - Copias de seguridad
  - Mecanismos de análisis forense (averiguar alcance, las actividades del intruso en el sistema y cómo entró).

Herramientas para la Seguridad

Cifrado de datos

Basado en criptografía. Se basa en la existencia de un algoritmo de cifrado/descifrado, normalmente conocido Ek() y Dk'(). La dificultad reside en la existencia de unas claves de cifrado (K) y descifrado (K') desconocidas.

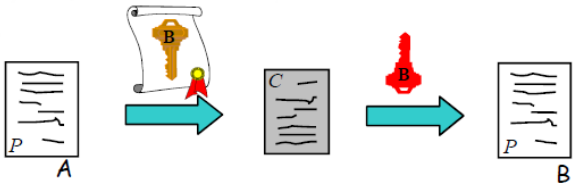


Cifrado simétrico

Se usa la misma clave para cifrar y descifrar mensajes en el emisor y receptor (K = K'), de manera que las dos partes deben acordar qué llave van a usar.
Algunos algoritmos son AES, DES, 3DES e IDEA (alternativa segura a DES).

Cifrado Asimétrico

También se conoce como cifrado de dos claves, ya que se usa un par de claves para el envío de mensajes. La llave pública se puede dar a cualquiera y la privada no puede verla nadie salvo el propietario. No hay 2 parejas de claves iguales y, conocida la llave pública K+, es computacionalmente imposible obtener la privada K-.
Si alguien usa su clave privada para cifrar se consigue identificación y autenticación del emisor y el mensaje puede ser descifrado por cualquiera usando su clave pública (firma electrónica) (Ka-(P) → K+a(P)).
Para mandar un mensaje garantizando confidencialidad, el emisor usar la clave pública del receptor para cifrar el mensaje, y únicamente éste puede abrirlo usando su clave privada (Kb+(P) → Kb-(P)).

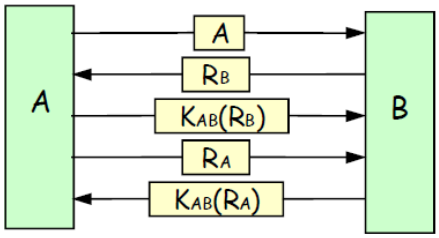


Como ejemplo esta RSA (firma digital), basado en álgebra modular y la función de euler para el cálculo de las claves pública y privada.

Autenticación y cifrado con clave secreta

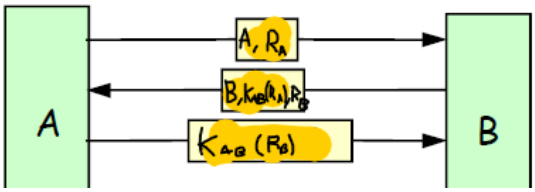
Autenticar consiste en verificar de forma fehaciente (sin fisuras) la identidad de las claves involucradas (“A es quien dice ser”).

Esquema de reto respuesta

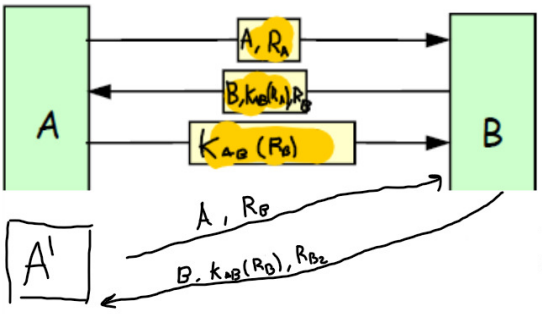


A dice que se quiere autenticar, B le envía un reto y A le envía la respuesta y su desafío y por último B le manda su respuesta

Se puede hacer más eficiente (usando sólo 3 mensajes):



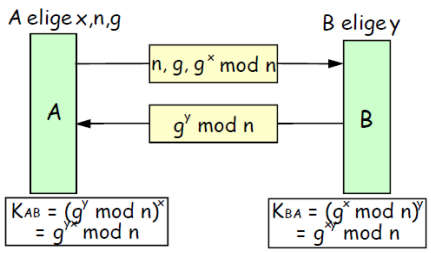
Problema: Se pueden sufrir ataques por reflexión



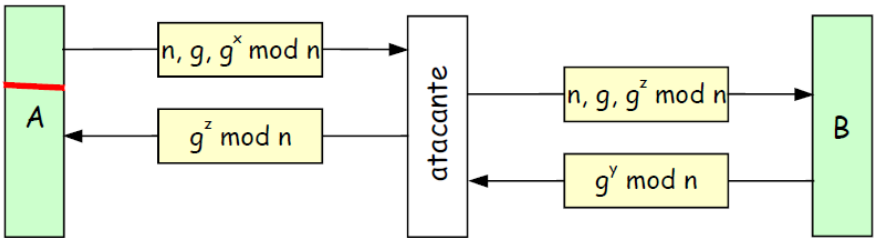
El atacante inicia la conexión y cuando B le manda el reto, abre otra conexión con él y le manda su mismo reto para que le mande la respuesta y acto seguido mandarsela a él de vuelta

Intercambio de Diffie-Hellman

Permite establecer una clave secreta entre dos entidades a través de una canal no seguro



Problema: puede sufrir ataque man-in-the-middle



Para evitar este ataque hay que hacer una autenticación previa a Diffie-Hellman.
Para más seguridad hay que aplicar esta a cada protocolo . La seguridad en las distintas capas va con parches, lo que genera más cabeceras.

Funciones Hash

Al llegar el mensaje M, se le aplica una función hash, obteniéndose H(M) ≠ M.
Es imposible obtener M a partir de su resumen H(M).
Algunos ejemplos de funciones Hash son MD5, SHA-1, SHA-512.

Hash Message Authentication Code (HMAC)

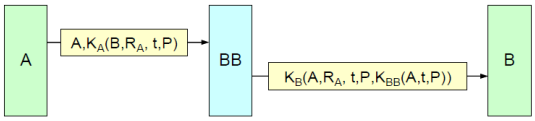
Garantiza integridad + autenticación M + H(K | M) pero para evitar ataques de extensión se usa M + H(K | H(K | M)) → se hace hash de la llave concatenada con el hash hecho a la llave concatenada con el mensaje.

Firma digital

Objetivos:

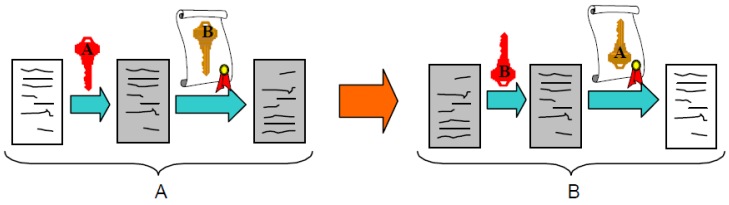
- El receptor pueda autenticar al emisor (el firmante)
- No haya repudio (irrenunciabilidad)
- El emisor (firmante) tenga garantías de no falsificación (integridad) por parte del destinatario

Firma digital con clave secreta (big Brother)



Firma digital con clave asimétrica (doble cifrado)

- Uno para proporcionar privacidad, con KpubB
- Otro, previo, para autenticación, con KpriA
- Para firmar, enviar KpubB(KpriA (T) →
- En el receptor KpubA (KpriB (KpubB(KpriA (T))))=T



- Debilidad: para garantizar el no repudio se necesita garantizar la asociación fehaciente e indisoluble de la "identidad A" con su "clave pública KpubA" (A ←→ KpubA) … ?
  esto se consigue con un "certificado digital"

Certificados digitales

Un certificado digital sirve para garantizar fehacientemente la asociación "identidad - clave pública".
Se necesita la intervención de una Autoridad de certificación (AC).

Una Autoridad de certificación (AC) es una entidad que sirve para garantizar la asociación entre identidad y sus claves:

- El usuario obtiene sus claves pública y privada
- Éste envía una solicitud, firmada digitalmente, a la AC indicando su identidad y su clave pública.
- AC comprueba la firma y emite el certificado solicitado:
  - Identidad de EZ, identidad usuario, clave pública del usuario, …
  - Todo ello firmado digitalmente con la clave privada de AC Con objeto de que el certificado no pueda falsificarse.

El formato de los certificados sigue principalmente la norma X.509, que tiene campos:

- Version
- Serial number
- Signature
- Issuer
- Validity period
- Subject name
- Public key

Protocolos seguros (implementación de mecanismos de seguridad)

Seguridad perimetral: Firewall + sistemas de detección de intrusiones (IDS) y de respuesta (IRS).

Seguridad en protocolos:

- Capa de aplicación:
  - PGP (Pretty Good Privacy) → Korig-(Kdest+(Ksecreta)): para seguridad en correo electrónico
  - SSH (Secure Shell)
- Capa de Sesión:
  - TSL (Transport Secure Layer, antes SSL) → HTTPS, IMAPS, SSL-POP
  - TSL → Handshake + Record Protocol (negociar + operar). Ofrece confidencialidad (Ksecreta negociada), autenticación para el servidor con K+ e integridad (HMAC)
- Capa de Red:
  - IPSec (VPN (Virtual Private Network)) → Permite la extensión segura de una red de área local.