ASI

Segunda Parte: Seguridad en S.I.

3º Ingeniería de Telecomunicaciones — UPV/EHU
"Under-promise and over-deliver."
Javier de Martín – 2016/17

1. Introducción

"*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*"

Amenaza[1]: Condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese un problema de seguridad.

Establecer un nivel de seguridad adecuado en un SI es complejo. Hay que definir los servicios a proporcionar, seleccionar las herramientas, monitorización constante...

Ataque: Cualquier acción que comprometa la seguridad de cualquier componente de un SI de una organización.

Servicios de Seguridad: Un proceso o equipo que lo contiene diseñado para detectar, prevenir o recuperarse de un ataque.

Mecanismos de Seguridad: Servicio de procesado o comunicaciones que aumenta la seguridad de los sistemas de procesado o transmisión de información de una organización. Se crean para protegerse de ataques contra la seguridad, y se hace uso de uno o varios mecanismos para proporcionar cada servicio.

Sevicios de seguridad de OSI son servicios provistos por una capa de un sistema de comunicaciones, asegurando la seguridad adecuada de los sistemas o transmisiones de datos definidos según la recomendación ITU-T X.800.

Los **mecanismos de seguridad OSI** son las técnicas o herramientas utilizadas para implementar un servicio de seguridad. Están diseñados para:

- **Prevenir** ataques que violan la política de seguridad de un sistema
- **Detectar** ataques de violación de la política de seguridad de un sistema.
- **Recuperarse** de un ataque contra la seguridad de un sistema.

No existe un único mecanismo capaz de proveer todos los servicios. Los mecanismos pueden ser clasificados como preventivos, detectivos y recuperables.

2. Fundamentos de Seguridad en los SI

Un **Sistema de Información** son los elementos[2] que contienen, transportan y sirven información para manipularla.

[1] Puede ser causada por usuarios, programas maliciosos, errores de programación, siniestros...

[2] Servidores, plataformas de usuario, aplicaciones, red...

2.1. Ataques

Un **ataque** es una acción contra la seguridad de un sistema que se deriva de una amenaza inteligente. Es un intento deliberado para eludir servicios de seguridad y la política de seguridad de un sistema. Es también cualquier actividad maliciosa que intenta recoger, interrumpir, denegar, degradar o destruir recursos de un Sistema de Información o información.

Un **ataque pasivo** se basa en la monitorización y atentan contra la confidencialidad. Difíciles de detectar ya que no realizan modificaciones en el sistema.

- **Divulgación de la información**: Se difunde la información obtenida.
- **Análisis de tráfico**: Si la información transcurre encriptada, se puede obtener de ahí información de la frecuencia y distribución del tamaño de la misma.

Un **ataque activo** implica la modificación o inserción de elementos en el sistema. Tienen características opuestas a los ataques pasivos. Tiene características opuestas a los ataques pasivos.

- **Usurpación de identidad**: Se simula ser una entidad distinta con otros privilegios.
- **Retransmisión**: Se vuelven a transmitir secuencias de información, capturadas previamente con objeto de producir un efecto desautorizado.
- **Modificación de mensajes**: Se modifica parte de un mensaje legítimo.
- **Denegación de servicios**: Trata de impedir o degradar el funcionamiento normal del sistema.

2.2. Servicios

Los **servicios de seguridad** en OSI son:

- Autenticación
- Control de Acceso
- Confidencialidad
- Integridad de datos
- No repudio

La **autenticación entre entidades pares** permite verificar que la entidad es quien dice ser, utilizado en las fases de establecimiento y transferencia de datos. La autenticación del origen de datos no proporciona protección frente a duplicación o modificación. Se emplea en tareas de autorización (concesión de derechos) y contabilidad (control de

El **control de acceso** permite proteger los recursos del sistema contra la utilización no autorizada. Para realizar el control de acceso es preciso identificarse. Define perfiles y granularidad.

La **confidencialidad** es la **protección frente a revelaciones** no autorizadas y ataques pasivos. Cuatro tipos:

- **Orientado a conexión** → datos transmitidos durante una conexión. TCP.
- **No orientado a conexión** → unidades simples. UDP.
- **De campo selectivo** → Campos específicos en una conexión o unidad de datos.
- **Flujo de tráfico** → Contra análisis de tráfico.

La **integridad de datos** es la **protección contra modificaciones** no autorizadas. Se dividen en función del objetivo a proteger (servicio de integridad orientado a conexión o no orientado a conexión) y en función al alcance de la herramienta (servicio con y sin recuperación[3]).

No repudio permite proteger contra las posibles negociaciones de acciones realizadas. Hay dos tipos:

- Con prueba de origen → Se puede asegurar que el mensaje ha sido enviado por el origen original.
- Con prueba de destino → Al emisor se le garantiza la recepción en el destino.

La **disponibilidad** especifica que los sistemas deben estar disponibles siempre[4].

2.3. Mecanismos

Los **mecanismos de seguridad de OSI** son:

- **Específicos**: Técnicas destinadas a facilitar un servicio[5].
- [6]: Pueden considerarse como aspectos de gestión de seguridad (relacionados directamente con el nivel de seguridad requerido)[7]

También es interesante considerar mecanismos a distintos niveles:

- **Mecanismos a nivel de Red**: Se autentica y cifra todo el tráfico de red, se protege a todas las aplicaciones, requieren la misma solución en todos los nodos, IPv6 e IPsec fueron diseñados con ello en mente. Hay soluciones parciales, entre routers de la organización VPN.
- **Mecanismos a nivel de Aplicación**[8]: Dado que no hay mecanismos globales, se buscan soluciones para cada una de las aplicaciones que nos interesa.

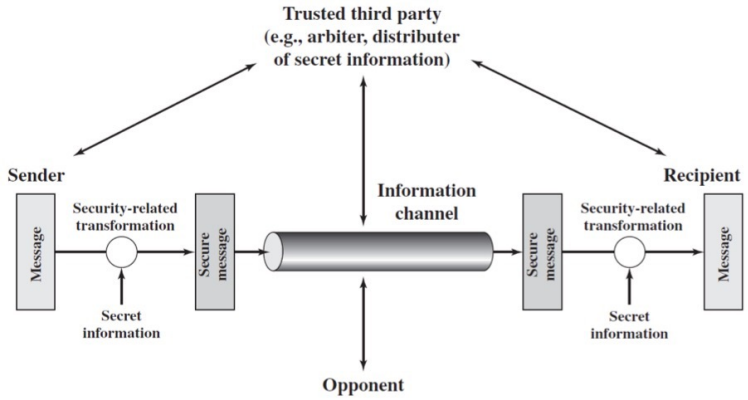


Figura 1: Modelo de Seguridad de Red

Explicar dibujo

Explicar dibujo

La NIST define la seguridad como la triada (figura 10) CIA: Confidentiality, Integrity y Availability:

[3]Si se nota que ha habido una modificación se puede pedir una retransmisión del mensaje original.

[4]Como un sistema no puede estar disponible siempre se utilizan sistemas redundantes o detección de fallos.

[5]Por ejemplo: Cifrado, firma digital, control de acceso, integridad, intercambio de autenticación, relleno de tráfico, control de encaminamiento y certificación

[6]Generalizados

[7]Por ejemplo: confianza, etiquetas de seguridad, detección, recuperación...

[8]PCP, SSH, HTTPS, SSL...

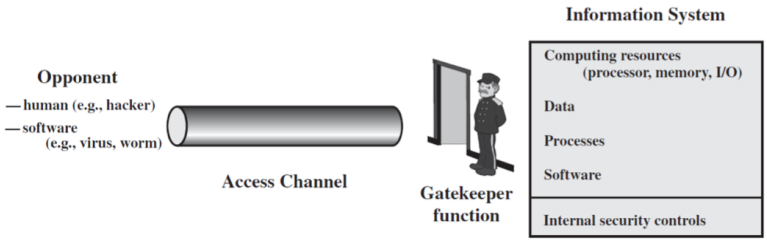


Figura 2: Modelo de Seguridad para Acceso a Red

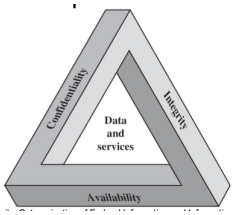


Figura 3: Triada de Seguridad

- **Confidencialidad**: Protección del acceso (o revelación) a la información solo para personas autorizadas, incluyendo medios para proteger privacidad e información de propietario. Una pérdida de confidencialidad supone la revelación no autorizada de información.
- **Integridad**: Protección frente a modificación o destrucción de información de forma no autorizada (incluye no repudio y autenticidad). Una pérdida de integridad supone la modificación o destrucción no autorizada de información.
- **Disponibilidad**: Asegurar el acceso y la utilización a tiempo y de forma confiable a la información. Una pérdida de disponibilidad supone la interrupción en el acceso o utilización de una información o sistema de información.
- **Autenticidad**: Propiedad de ser genuino y con capacidad para ser verificado y confiable. Confiabilidad en la validez de una transmisión, de un mensaje o del originador de un mensaje. Que se pueda verificar que los usuarios son quienes dicen ser, o que las entradas a un sistema proceden de una fuente confiable.
- **Contabilidad**: Como no es posible que los sistemas sean completamente seguros, las partes autorizadas deberían disponer de mecanismos para trazar eventos de seguridad. Los sistemas deben almacenar registros de sus actividades para permitir análisis forenses posteriores para ayudar en la resolución de conflictos. Proporciona no repudio, disuasión, detección y prevención de intrusión, y posibilita recuperación y acciones legales posteriores.

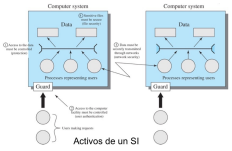


Figura 4: Activos, amenazas y ataques

Explicar dibujo

- **Amenazas**: "*Condición del entorno de sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad*".

- **Ataque**: "*Un ataque es la realización de una amenaza*".

Una **amenaza a la seguridad** es la posibilidad de violación de seguridad, que existe cuando una entidad, circunstancia que puede causar daños. Un peligro que se deriva de una posible explotación de una vulnerabilidad. Para estudiar los tipos de amenazas se suele partir de la consideración que la función de un SI es proporcionar información, se considera que hay un flujo de información de una fuente a un destino.

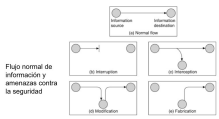


Figura 5: Amenazas a la seguridad

Explicar dibujo

3. Técnicas Criptográficas

3.1. Introducción a la criptografía

- **Esteganografía** tiene como objetivo ocultar la existencia de un mensaje.
- **Criptografía**: Objetivo es ocultar el significado del mensaje, el proceso se conoce como codificación.
- **Criptología**: Ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones. Criptografía + Criptoanálisis.
- **Criptografía**: Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Tradicionalmente asociada sólo al cifrado. Actualmente es parte de la criptología que se encarga del estudio de los algoritmos, protocolo criptográficos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y las entidades que se comunican.

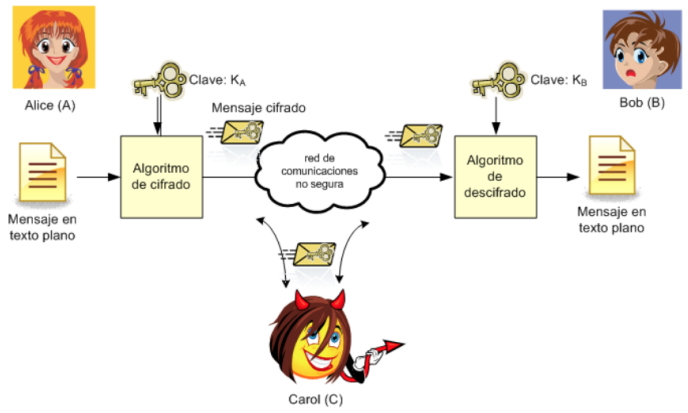


Figura 6: Fundamentos de la criptografía

Elementos clave del sistema: Terminar

- **Texto en claro**:
- **Texto cifrado**:
- **Clave de cifrado**: K_A
- **Clave de descifrado**: K_B

Los **sistemas criptográficos** se caracterizan en función de:

- Tipo de operaciones utilizadas para transformar el plaintext en ciphertext: sustitución y transposición.
- Número de claves utilizadas: simétrica y asimétrica.
- Forma en la que se procesa el plaintext: Bloque y stream.

Tipos básicos de cifrado en función del tipo de operaciones:

- Sustitución: Las unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular. Las unidades pueden ser una sola letra o grupos más grandes. El receptor descifra el texto realizando la operación inversa. Hay varios tipos:
  - Simple: Opera sobre letras simples. Hay mono alfabético, si la sustitución es simple para todo el mensaje, y polialfabético, si utiliza diferentes sustituciones en diferentes partes de un mensaje.
  - Polígráfico: Opera sobre grupos de letras.
- Transposición: Las unidades del texto plano son cambiadas usando una ordenación diferente y normalmente bastante compleja, pero las unidades en sí mismas no son modificadas.

Criptografía de **clave secreta o simétrica**: Se utiliza la misma clave para cifrar y descifrar.

$$K_A = K_B = K_{AB} \quad K_{AB}(K_{AB}(m)))$$

La clave es **secreta** (K_{AB}) es conocida por los dos participantes de la comunicación.

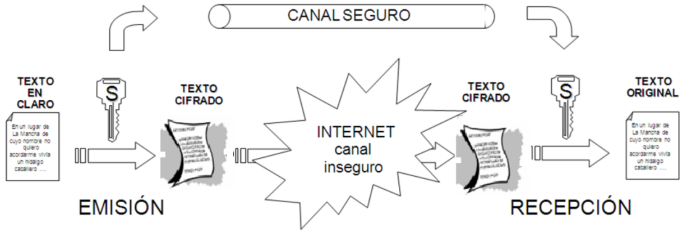


Figura 7: Criptografía de clave secreta o simétrica

Terminar

Criptografía de **clave pública o asimétrica**: Cada usuario cuenta con un par[9] de clave pública (K^+)/privada (K^-). Dada la clave pública (K^+), es computacionalmente inviable obtener la clave privada (K^-). La clave privada es secreta y por tanto, conocida únicamente por el propietario legítimo de la misma, mientras que la clave pública es pública, y por tanto conocida por todos.

Terminar

Todo lo que se cifra con la clave pública únicamente puede ser descifrado con la correspondiente clave privada y vice-versa.

$$K^+(K^-(m))) = m \quad \text{ó} \quad K^-(K^+(m))) = m$$

Para garantizar la confidencialidad de los mensajes enviados, todos los emisores han de cifrar los mensajes con clave pública del usuario de destino (K_X^+), conocida por todos, y sólo será el usuario de destino que podrá descifrar el mensaje con su clave privada (K_X^-). El proceso sería el siguiente:

[9] Por ejemplo, para un usuario Alice su par sería K_A^+/K_A^-.

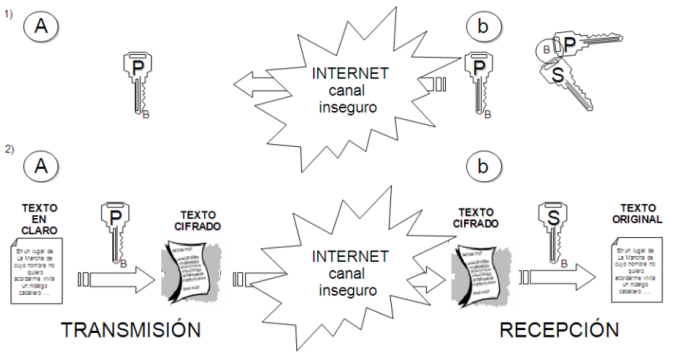


Figura 8: Criptografía de clave pública o asimétrica

$$\text{Alice:} \quad m \rightarrow K_B^+(m)$$
$$\text{Bob:} \quad K_B^-\{K_B^+(m)\} = m$$

Criptoanálisis es la parte de la criptología que se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. Buscar romper o forzar el código. Hay varios tipos de ataques según el conocimiento previo del atacante:

- **Ataques *ciphertext-only***: Cuando sólo se dispone del texto cifrado. Por ejemplo: Fuerza bruta, análisis de frecuencias o método Kasiski.
- **Ataque *known-plaintext***: El atacante conoce el texto original. En ocasiones, el atacante conoce una parte del texto o alguna palabra probable.
- **Ataque *chosen-plaintext***: El atacante tiene la capacidad de definir un texto y obtener el correspondiente texto cifrado. El objetivo es poder descifrar textos que se descicfren e ese descifrador. Si un sistema es seguro frente a ataques *chosen-plaintext* también es seguro frente a ataques *known-plaintext* y *ciphertext-only*.

3.2. Cifrado

El **cifrado** es la puesta en clave (*ciphertext*) de un texto (*plaintext*) mediante una función parametrizada por una clave. Previene ataques contra la confidencialidad.

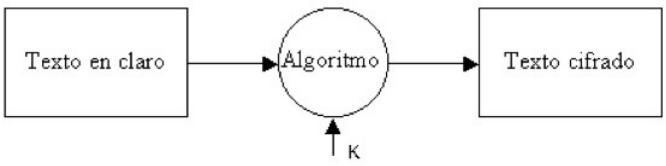


Figura 9: Cifrado

El criptoanálisis es la ciencia que estudia los sistemas que permiten desbaratar textos cifrados y obtener los correspondientes textos en claro.

Los algoritmos de cifrado más antiguos hacen uso de criptografía simétrica.

Tamaño de claves para proporcionar un nivel de seguridad similar en algoritmos de cifrado. **Tabla de bits cifrado no entiendo**

3.3. Códigos de Autenticación de Mensaje (MAC)

Permiten proteger la integridad y autenticidad de origen de los mensajes. Comprueban que el origen del mensaje es quién dice ser y que dicho mensaje no ha sido modificado durante su transmisión. Pueden considerarse sinónimos, si un mensaje es modificado durante su transmisión, ya no procede de su emisor légitimo sino de quien lo modificó.
A veces puede ser necesario garantizar la integridad del mensaje pero no su confidencialidad.

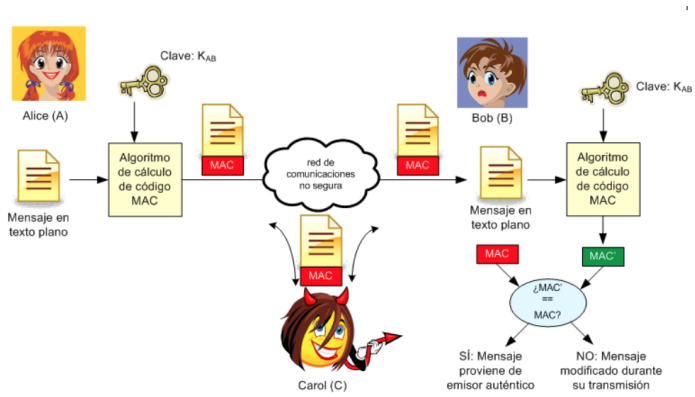
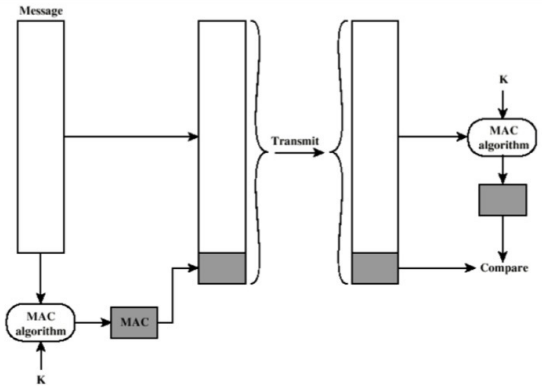


Figura 10: Autenticación de Origen

Explicar

Una **función *hash***[10] h es una función que mapea cadenas de bits de longitud arbitraria a cadenas de longitud fija de n bits (huella dactilar), es una función resumen y es de un único sentido. Dada una función hash h y una entrada x, la salida $h(x)$ es computacionalmente sencilla de calcular. Se puede ir del texto al resumen pero en sentido inverso es imposible, una función hash no es reversible. Dado un valor y, es computacionalmente inviable encontrar un valor de x' de forma que $h(x') = y$ por tanto no habrá colisiones.

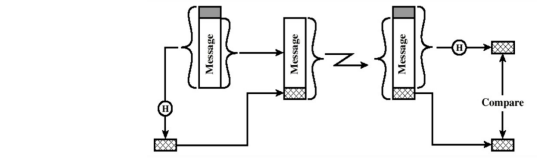
MAC (*Message Authentication Code*) es un código que permite la autenticación de mensajes mediante técnicas criptográficas de clave simétrica. Los algoritmos de MAC toman como entrada dos parámetros (mensaje y clave simétrica) y generan una salida de longitud fija con la característica de que es computacionalmente inviable producir la misma salida sin conocer la clave.



Terminar

Un **ejemplo de código MAC** es HMAC (*Hash-based Message Authentication Code*) y es un tipo específico de códigos MAC, el algoritmo utilizado para calcular el código MAC se basa en la utilización de funciones hash en lugar de, por ejemplo, algoritmos de cifrado.

[10] Por ejemplo los códigos CRC



Características de los códigos de autenticación de mensajes:

- Compresión: Mapean una entrada de longitud fija finita arbitraria a una salida de longitud finita fija.
- Facilidad de cómputo: Dada una función hash h y una entrada x, la salida $h(x)$ es computacionalmente sencilla de calcular.
- Unidirecional (no reversible): Dado un valor y, es computacionalmente inviable encontrar un valor x' de forma que $h(x') = y$.
- Sin colisiones: Es computacionalmente inviable encontrar dos entradas x y x' distintas de forma que $h(x) = h(x')$.

3.4. Firmas Digitales

Técnica criptográfica análoga a las firmas hechas a mano. Garantiza la integridad o autenticación de origen de un mensaje. Es verificable, no falsificable. El destinatario puede demostrarle a alguien que el origen, y no otra persona (incluyendo el destinatario), ha firmado el documento. Resumen (*hash*) del mensaje cifrado.

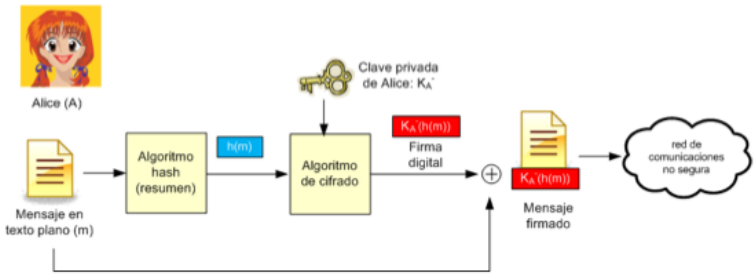


Figura 11: Generación de firma digital

La verificación separa el mensaje de la firma. Con el algoritmo de descifrado y la clave pública de A se extrae el resumen. ¿Por qué tiene que haber un resumen criptográfico? Para evitar conseguir dos resúmenes que sean iguales.

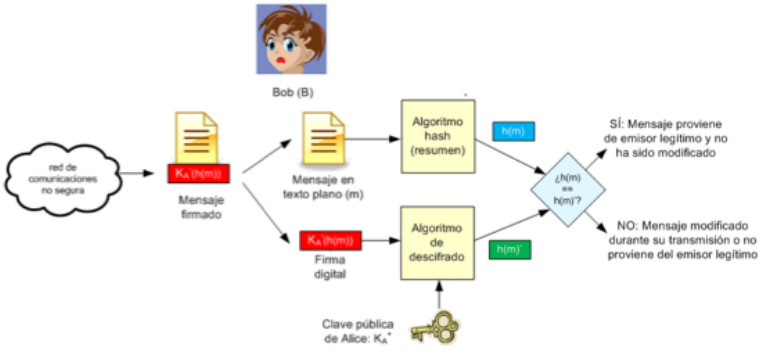


Figura 12: Verificación de firma digital

No se puede autenticar el origen con el hash.

Crypto Primitive Security Goal	Hash	MAC	Digital Signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-Repudiation	No	No	Yes
Kind of Keys	None	Claves simétricas	Claves asimétricas

3.5. Frescura de Mensajes

Incluso cifrando un mensaje y autenticándolo (mediante código MAC o firma digital) todavía es posible que un atacante intercepte un mensaje legítimo y lo repita más tarde haciéndose pasar por el emisor legítimo (ataque de repetición de mensajes). Es necesario garantizar la frescura de los mensajes.

Un **ataque de repetición de mensajes** consiste en que el destinatario cree que ha recibido un nuevo mensaje del origen cuando en realidad se trata de un mensaje antiguo repetido por un intermediario.

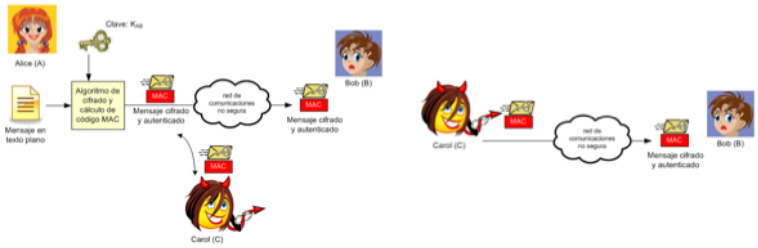


Figura 13: Ataque de Repetición de Mensajes

Mecanismos de Frescura:

- **Sellos de tiempo**: Genera datos que identifican el momento en el que se crearon los datos. Pueden estar basados en la utilización de relojes o en sellos de tiempo lógicos (números de secuencia). ¿Cómo funciona? El generador del mensaje incluye la hora/fecha de generación del mensaje (sello de tiempo) en el mensaje original. Cuando el destinatario recibe el mensaje, compara el sello de tiempo incluido en el mismo con la hora/fecha actual. Si el retardo del mensaje es mayor que el retardo normal en la red de comunicaciones se descarga el mensaje (se trata de un mensaje repetido). Tiene una desventaja, tanto el origen como el destino tienen que mantener sus relojes sincronizados.
- **Nonces/Testigos**: Número que se introduce para una utilización única (one-time identification). Normalmente, es un número generado aleatoriamente. Refleja la frescura si asumimos que se generan números que no han sido usado antes. Son valores únicos e impredecibles. A $N1$ se le denomina reto (*challenge*)

Figura 14: Nonces

- **Unilateral Symmetric Key**:
  - Autenticación con sello de tiempo generado por A: Origen y destino tienen los relojes sincronizados, el destino sólo acepta mensajes durante un cierto período de tiempo.

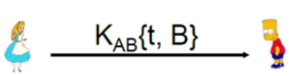


Figura 15: Autenticación con sello de tiempo generado por el origen

  - Autenticación unilateral con *nonce*:
- **Mutual Symmetric Key**: Con nonces

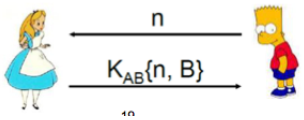


Figura 16: Autenticación unilateral con nonce

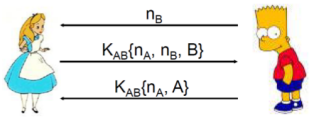


Figura 17: Mutual Symmetric Key con nonces

3.6. Distribución de Claves

Está obligatoriamente ligado al proceso de autenticación. No tiene sentido establecer una clave con un usuario no autenticado, *¿Es realmente el usuario con el que me quiero comunicar?*. No tiene sentido autenticar a un usuario y no establecer una clave, *¿Una vez finalizado el proceso de autenticación cómo sé que el usuario con el que me estoy comunicando es el mismo previamente autenticado?*.

La **criptografía de clave simétrica**: Tiene varios problemas, *¿Cómo pueden dos entidades establecer una clave secreta compartida a través de la red no segura?* Se requiere una clave por cada par de usuarios. Para n participantes hay $n\frac{n-1}{2}$ claves. La solución es el centro de distribución de claves (*KDC*) actuando como intermediario en el que confían las dos entidades que quieren establecer una clave compartida entre ambas.

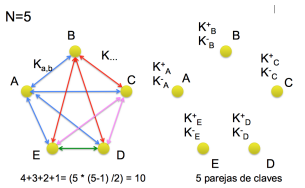


Figura 18: Comparativa del número de claves

Explicar dibujo

En el **centro de distribución de claves** (KDC) cada usuario registrado en el sistema comparte una calve secreta con el KDC:

- $K_{A,KDC}$: Clave compartida entre Alice y el KDC.
- $K_{B,KDC}$: Clave compartida entre Bob y el KDC.

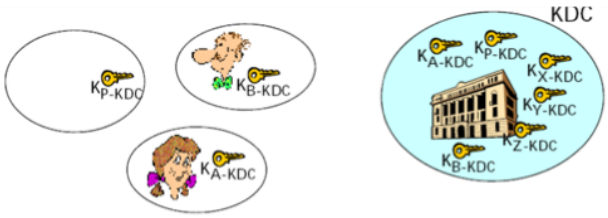


Figura 19: Key Distribution Center

KDC, establecimiento de clave K' como clave de sesión para comunicación segura entre origen y destino.

Kerberos es uno de los sistemas de distribución de claves más populares. El KDC consta de 2 servidores, *Authentication Server* (AS) y *Ticket Granting Server* (TGS). En cuanto a **escalabilidad** permite la existencia de diferentes dominios (*realms*). Los KDCs de los diferentes dominios establecen asociaciones de seguridad entre sí. La **autenticación** de usuario se realiza en 2 fases:

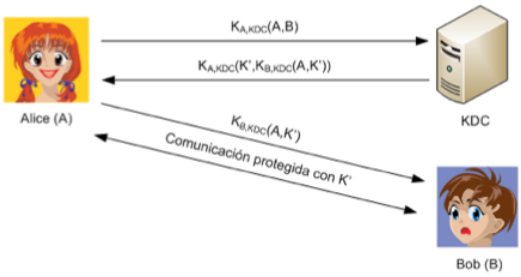


Figura 20: Establecimiento de una clave

- Fase de autenticación: El usuario se autentica frente al AS de Kerberos. Obtiene un *Ticket Granting Ticket* (TGT), el cual es una especie de ticket maestro que identifica al usuario como ya autenticado.
- Fase de emisión de tickets: El usuario obtiene del TGS de kerberos un ticket de servicio, el cual es la credencial que ha de presentar al usuario remoto frente al que se quiere autenticar.

Este mecanismo de autenticación permite implementar mecanismos de *Single-Sign On*, gracias al TGT el usuario puede obtener todos los tickets de servicio que desee sin volver a autenticarse frente al AS.

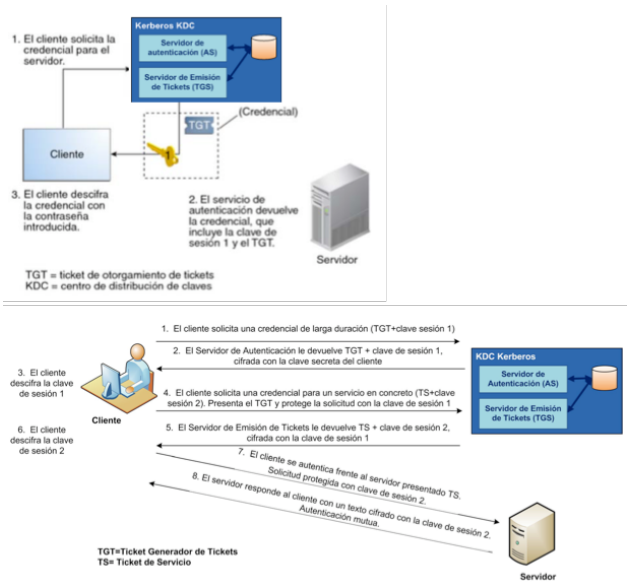


Figura 21: Operación de Kerberos

COmentar con texto la figura

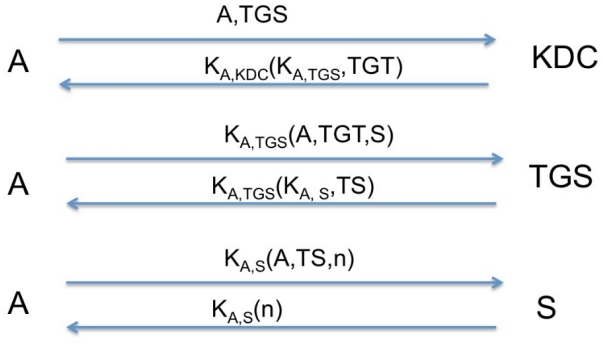


Figura 22: Operación de Kerberos

Comentar la imagen

En KDC se demuestra la identidad una vez. En TGS se solicitan los servicios con el ticket.
Si tienes un certificado por ti mismo significa que eres una autoridad certificadora.

Primera flecha, Viaja en claro A le dice al KDC que quiere hablar con el TGS. Le devuelve un ticket y la clave $A - TGS$.
A le envía al TGS su ticket y servicio que solicita.

Un **certificado** es una identidad con una clave pública firmados por una autoridad.

La criptografía de clave pública tiene un problema, *Cuando Bob obtiene la clave pública de Alice, ¿Cómo puede estar seguro de que es realmente la clave pública de Alice y no de otro usuario intentando hacerse pasar por Alice?* Se puede dat un ataque *Man in the Middle*.

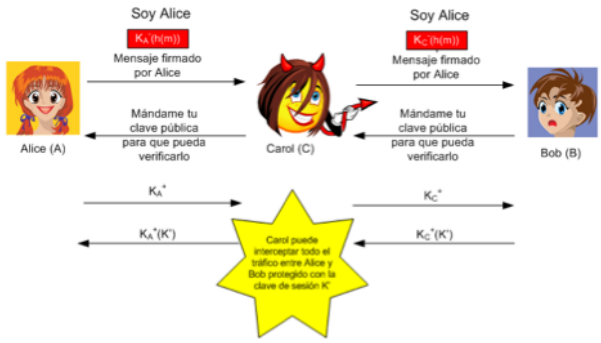


Figura 23: Man in the Middle

La **solución** a los positbles ataques MiTM es la CA (*Certification Authority*). Está basado en el uso de Autoridades de Certificación y servicios de directorio. Un certificado digital es un documento digital firmado por una Autoridad de Certificación de confianza que asocia una clave pública a una identidad. Si dos usuarios disponen de certificados emitidos por diferentes CAs es preciso construir una vía de certificación. Claves públicas de CAs dentro de los navegadores.

Un **certificado digital** (X.509) es un documento firmado por una Autoridad de Ceritficación de confianza que asocia una clave pública a una identidad.

Si dos usuarios disponen de certificados emitidos por diferentes CAs es preciso construir una **vía de certificación**.

Un usuario A $E^-_{AC_1}\{A, E^+_A\}$ con una AC1 y uno B $E^-_{AC_2}\{B, E^+_B\}$ con una AC2 certificados por dos autoricades diferentes ya que uno no le vale al del otro, entonces una autoridad certificadora tiene que verificar la identidad de la otra autoridad verificadora. Por ejemplo para el usuario A, tiene que verificar la identidad de la AC2 como $E^-_{AC_1}\{AC2, E^+_{AC2}\}$.

Una CA necesita una **prueba de identidad**[11] de un E(persona, router) para poder crear un certificado[12] que vincule a E a su clave pública.

El certificado será la pareja identidad clave pública firmada por la autoridad certificadora:

$$E^-_{AC} = \{A, E^+_A\}$$

Cuando un usuario B quiere comunicarse con un usuario A le solicita la clave pública. Obtiene el certificado de A, aplica la clave pública CA al certificado de A.
Certificados cruzados. Dos usuarios A y B con certificados emitidos por `CA1` y `CA2` no pueden verificar los certificados de manera segura por que no tienen los certificados de la otra CA.

[11] Clave pública y la clave pública firmada con la clave privada $\rightarrow E^-_{AC}\{A, E^+_A\}$
[12] Este certificado contiene la clave pública de E firmada digitalmente por CA

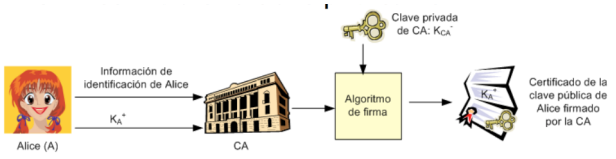


Figura 24: Emisión de certificados por la CA

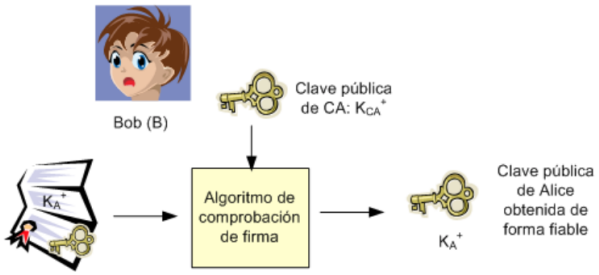


Figura 25: Petición de B a A por su certificado

- `A` dispone de:
  - Certificado de `CA1`: $E^-_{CA1}\{CA1, E^+_{CA1}\}$
  - Certificado de `B` emitido por `CA2`: $E^-_{CA2}\{B, E^+_B\}$
- `B` dispone de:
  - Certificado de `CA2`: $E^-_{CA2}\{CA2, E^+_{CA2}\}$
  - Certificado de `A` emitido por `CA1`: $E^-_{CA1}\{A, E^+_A\}$

El protocolo Diffie-Hellman es un **protocolo de establecimiento de claves** entre partes que no han tenido contacto previo utilizando un canal inseguro y de manera anónima (no autenticada). Se emplea como medio para acordar claves simétricas que se emplearán para el cifrado de una sesión. A pesar de no ser autenticado provee las bases para protocolos autenticados. Está sujeto a ataque de hombre de en medio por tanto habrá que usar una autenticación por encima.

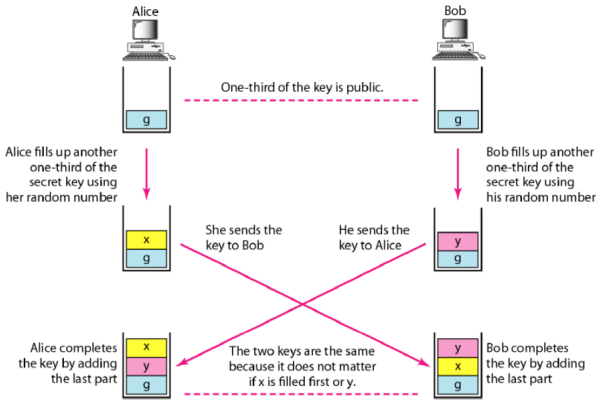


Figura 26: Protocolo Diffie-Hellman

Explicación: Existe una parte común `g`

3.7. Criptografía Simétrica y Asimétrica

La **criptografía simétrica** tiene un espacio de claves ≥ 128 bits, la vida de las claves es muy corta, la velocidad de firma es muy alta, la seguridad reside en la de la propia clave y el tamaño del mensaje no importa[13].

Para la **criptografía asimétrica** el espacio de claves es ≥ 1024 bits[14], la vida de éstas es larga, la velocidad de la firma es lenta, la seguridad

[13] Con algoritmos de bloque se puede firmar todo lo que sea
[14] Tamaño en bits que tiene el entero resultado de multiplicar dos números primos grandes

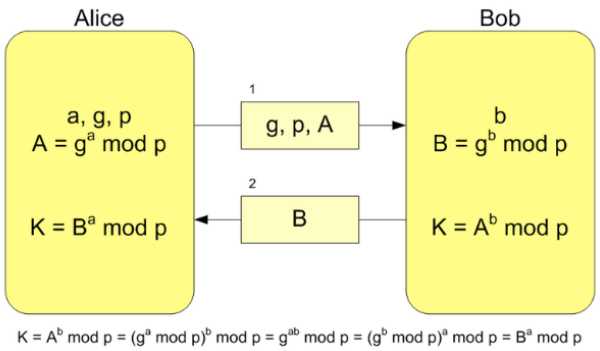


Figura 27: Funcionamiento del Protocolo Diffie-Hellman

reside en la dificultad computacional de encontrar la clave privada a partir de la clave pública y el tamaño del mensaje es menor que la longitud de la clave[15].

En la práctica se usa **criptografía híbrida** que utiliza dos algoritmos:

- Algoritmo de calve pública: Es más seguro y se usa para el cifrado en el envío de la clave simétrica.
- Algoritmo de clave simétrica: Se utiliza en el cifrado del mensaje y reduce el coste computacional.

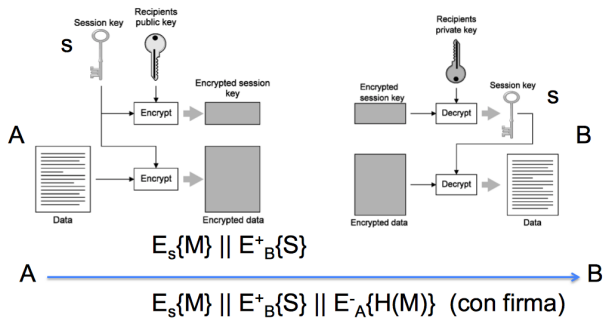


Figura 28: Funcionamiento de la criptografía híbrida

Se genera una clave S que se usa para cifrar el mensaje M. La clave S se firma con la pública de B certific. Tiene un problema ya que no se firma y se desconoce quién lo envía, si se quisiera firmar habrá que añadir el hash del mensaje crifrado con la clave privada del origen.

Si dicen que A y B tienen certificado están diciendo que la correspondencia entre clave pública y propietario están verificadas, por tanto no puede haber ataque de MITM.

3.8. Seguridad en SI

3.8.1. Seguridad en Dispositivos Finales

La seguridad en equipos finales se consigue utilizando un SO seguro, eligiendo buenas contraseñas, firewalls...

3.8.2. Seguridad en Comunicaciones

Implicaciones de la seguridad en cada capa:

- **Nivel de Enlace**: Relevante en caso de comunicaciones inalámbricas. IEEE 802.1X separa la autenticación de la autorización. Los componentes son el suplicante (Cliente Wi-Fi), Autenticador (AP Wi-Fi) y el Servidor de Autenticación (Servidor independiente o en el AP).
- **Nivel de Red** (IP): Confidencialidad en la capa de red (cifrado de datagramas IP), autenticación en la capa de red[16] y asociación de seguridad[17].
- **Nivel de Transporte** (SSL/TLS): En navegadores, como servicios de seguridad ofrece la autenticación del servidor, cifrado de datos y la autenticación del cliente.
- **Nivel de Aplicación**: No hay mecanismos globales por lo que se buscan soluciones específicas para cada aplicación.

Seguridad perimetral (cortafuegos) aísla la red interna de una organización de la red Internet, permitiendo que algunos paquetes pasen y bloqueando otros. Tienen limitaciones que hay que tener en cuenta.

La red interna conectada a Internet a través de un router cortafuegos. El router filtra paquete por paquete y se toma decisión de envío o rechazo del paquete en función de distintos parámetros [18].

Existen otros mecanismos de seguridad perimetral como: IDSs/ISPs, balanceadores, proxys web, antivirus, VPNs...

3.9. Situación Actual de la Seguridad

Un **ataque a la seguridad** es cualquier acción deliberada cuyo objetivo sea violar o comprometer la seguridad de un sistema[19].

3.10. Gestión de la Seguridad

Políticas de seguridad, la seguridad se alcanza en base a 3 procesos:

- Prevención (tratar de evitar que ocurra): Cortafuegos, antivirus, VPNs, NAT...
- Detección (detectar si a pesar de todo sucede): Sistemas de detección de intrusión
- Reacción (cómo reparo el daño y recupero el control): Planificación de acciones ante ataques o desastres.

Son necesarias las **políticas de seguridad**, plasmado en un documento que describe las relaciones permitidas entre sujetos y objetos.

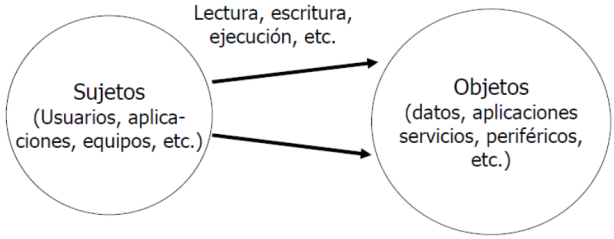


Figura 29: Políticas de seguridad

Técnicas relacionadas con el estudio de la seguridad: análisis de riesgos, análisis de metodologías, planes de contigencia y recuperación...

[15] Si por ejemplo el espacio de claves es de 1024 bits se pueden firmar mensajes de como máximo 128 bits

[16] El equipo destino puede autenticar la IP origen.

[17] Relación en un solo sentido entre emisor y receptor, si el intercambio fuera en dos sentidos se necesitarían 2 asociaciones de seguridad

[18] IPs origen y destino, puerto UDP o TCP, bits TCP SYN o ACK...

[19] Spyware, adware, MiTM, sniffing, phishing...