ASI

Segunda Parte: Seguridad en S.I.

3º Ingeniería de Telecomunicaciones — UPV/EHU

"Under-promise and over-deliver."

Javier de Martín – 2016/17

Parte 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.

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.

Los mecanismos de seguridad OSI están diseñados para:

- Prevenir
- Detectar
- Recuperarse

Los mecanismos pueden ser clasificados como preventivos, detectivos y recuperables.

Fundamentos de Seguridad en los SI

Ataques

Un **ataque pasivo** se basa en la monitorización y estudio del sistema y atentan contra la confidencialidad. Fáciles 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.

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

- Usurpación de identidad
- Retransmisión
- Modificación de mensajes
- Denegación de servicios.

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 recursos).

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

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.

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[1]).

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.

Mecanismos

Los mecanismos de seguridad de OSI son:

- Específicos: Técnicas destinadas a facilitar un servicio, por ejemplo: cifrado, firma digital, control de acceso, integridad, intercambio de autenticación, relleno de tráfico, control de encaminamiento y certificación.
- Generalizados: Pueden considerarse como aspectos de gestión de seguridad (relacionados directamente con el nivel de seguridad requerido), por ejemplo: confianza, etiquetas de seguridad, detección, recuperación...

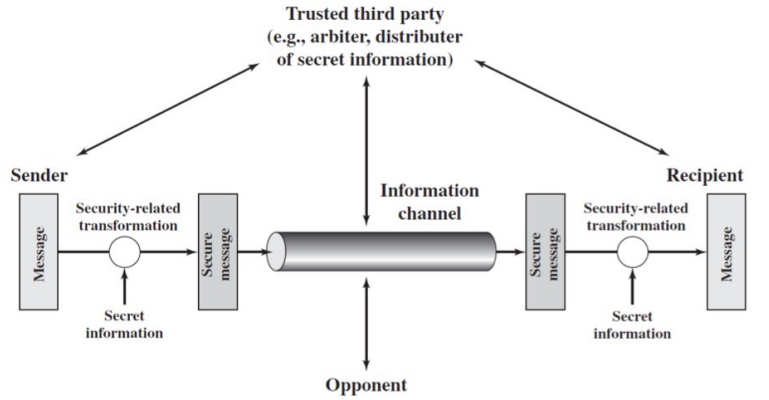
También es interesante considerar mecanismos a distintos niveles:

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

- 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: Dado que no hay mecanismos globales, se buscan soluciones para cada una de las aplicaciones que nos interesa.

Modelo de seguridad de red



La NIST define la seguridad como la triada CIA: Confidentiality, Integrity y Availability:

- Confidencialidad: Protección del acceso (o revelación) a la información solo para personas autorizadas, incluyebndo 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 inforamción de forma no autorizada (incluye no repudio y autenticidad). Una pérdida de integridad supone la modificación o destrucción no autorizada de información.

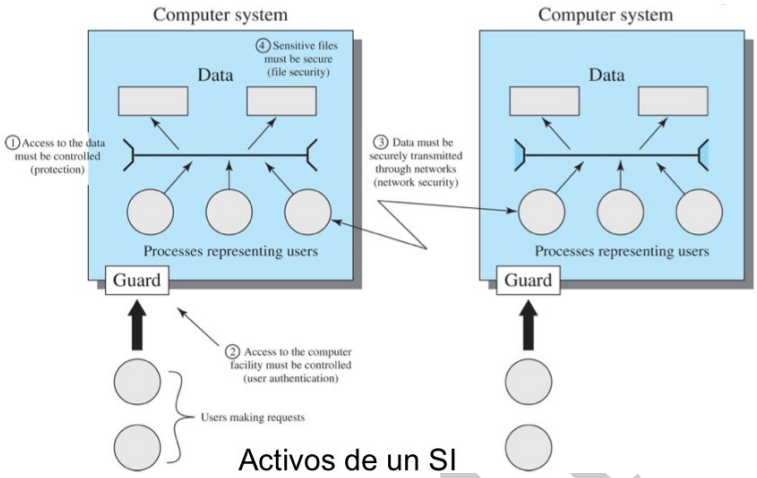
- Disponibilidad: Asegurar el acceso y la utilización a tiempo y de forma confiable a la información. Una pérdida de disponibilidad supone la interrupción en el acceso o utilización de una información o sistema de información.

- Autenticidad: Propiedad de ser genuino y con capacidad para ser verificado y confiable. Confiabilidad en la validez de una transmisión. 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 reuperación y acciones legales posteriores.

Activos, amenazas y ataques

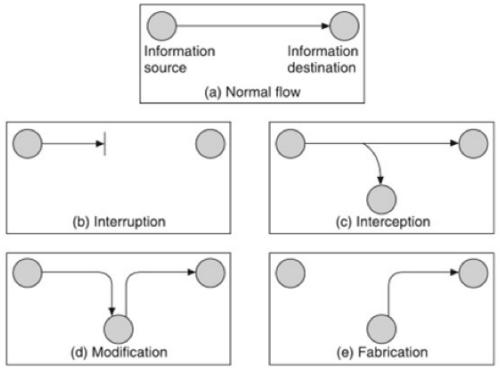


- **Amenazas**: "*Condición del entorno de sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad*".

- **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.

Flujo normal de información y amenazas contra la seguridad



Técnicas Criptográficas

Introducción a la criptografía

- **Esteganografía** tiene como objetivo ocultar el 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 adecuados. Tradicionalmente asociada sólo al cifrado.

Elementos clave del sistema: Texto en claro y texto cifrado, algoritmo de cifrado/descifrado y clave de cifrado (K_A) y 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 sóla 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.
  - Poligráfico: 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.

Criptografía de clave pública o asimétrica: Cada usuario cuenta con un par de clave pública (K^+)/privada (K^-). Dada la clave pública, es computacionalmente inviable obtener la clave privada. 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.
Todo lo que se cifra con la clave pública únicamente puede ser descifrado con la correspondiente clave privada y vice-versa.

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

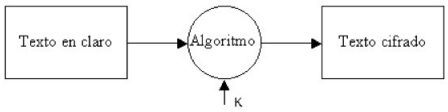
Para garantizar la confidencialidad de los mensajes enviados, todos los emisores han de cifrar los mensajes con clave pública del usuario de destino y sólo será el usuario de destino que podrá descifrar el mensaje.
Criptoanálisis es la parte de la criptología que se dedica al estudio de sistemas criptográficos 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*.

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.

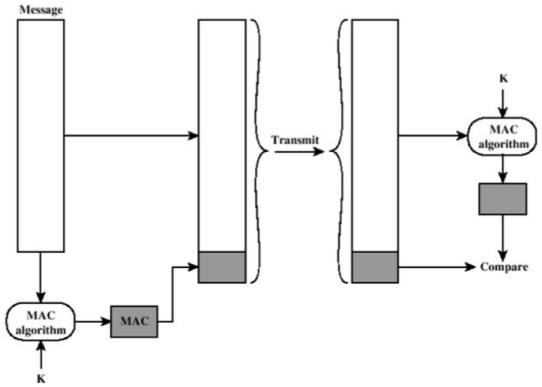


Códigos de Autenticación de Mensaje (MAC)

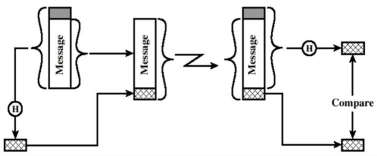
Permiten proteger la integridad y autenticidad de origen de los mensajes. Comprueban que el origen del mensaje es quién dice ser y que dicho mensaje no ha sido modificado durante su transmisión. Pueden considerarse sinónimos, si un mensaje es modificado durante su transmisión, ya no procede de su emisor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

Una **función *hash*** 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. Se puede ir del texto al resumen pero en sentido inverso es imposible.

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.



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.



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 $h(x) = h(x')$.

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.

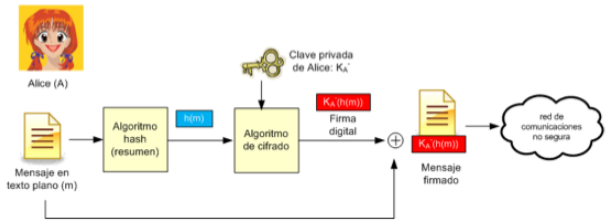


Figura 1: Generación de firma digital

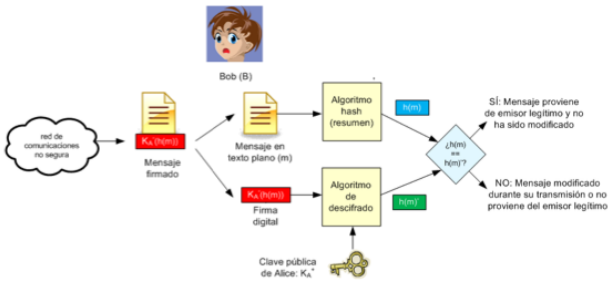


Figura 2: Verificación de firma digital

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.

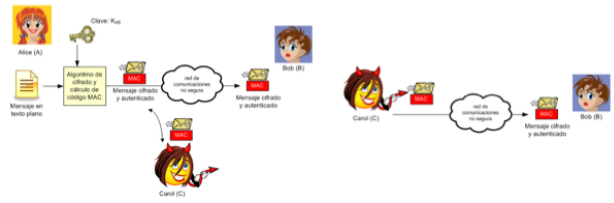


Figura 3: Ataque de Repetición de Mensajes

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**: 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 4: 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.

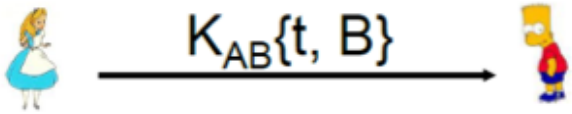


Figura 5: Autenticación con sello de tiempo generado por el origen

  - Autenticación unilateral con *nonce*:

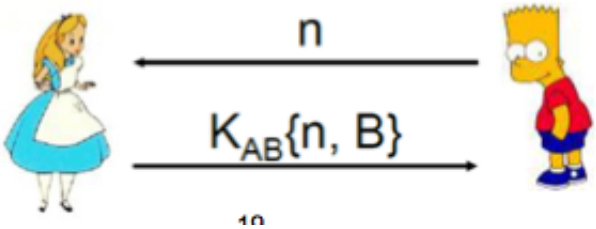


Figura 6: Autenticación unilateral con nonce

- **Mutual Symmetric Key**: Con nonces

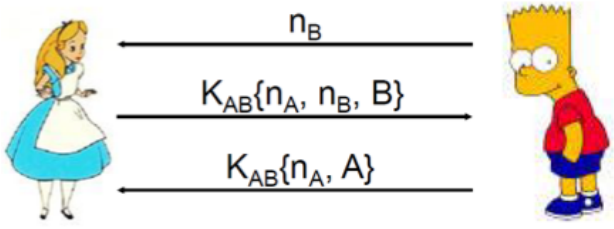


Figura 7: Mutual Symmetric Key con nonces

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.

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.

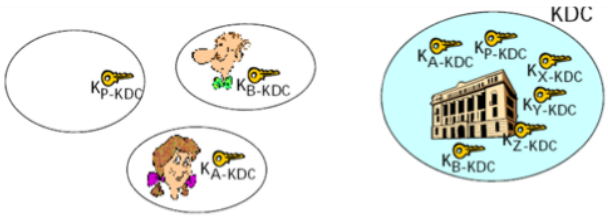


Figura 8: Key Distribution Center

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

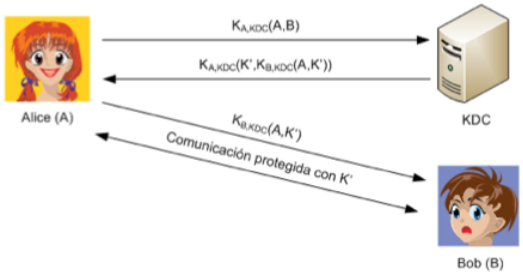
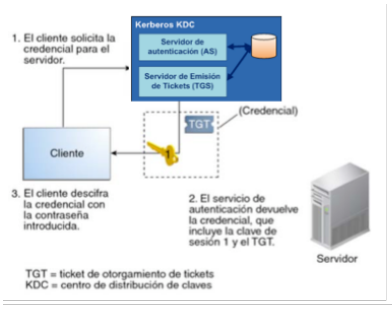


Figura 9: Establecimiento de una clave

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:

- 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.
La criptografía de clave pública tiene un **problema**. Cuando el destino obtiene la clave pública del origen, ¿cómo puede estar seguro de que es realmente la clave pública del origen y no de otro usuario haciéndose pasar por él? → Ataque *Man in the Middle*.



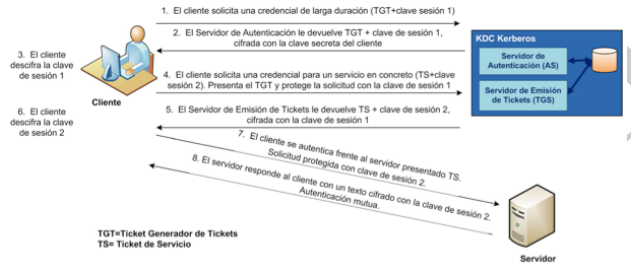


Figura 10: Operación de Kerberos

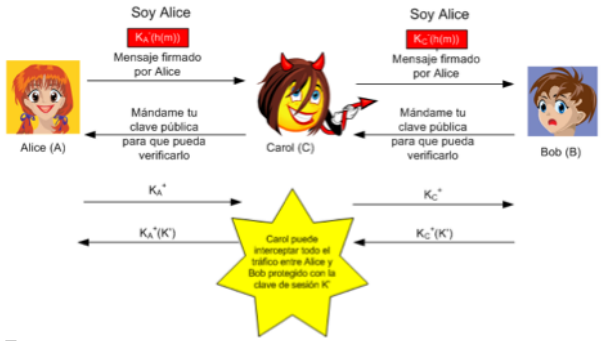


Figura 11: Man in the Middle

La **solución** 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.

Seguridad en SI

Situación Actual de la Seguridad

Gestión de la Seguridad

Parte 2

Parte 3

Parte 4