CUIA 21/22 - Tema 5: Seguridad

En un sistema de Computación Ubicua gran cantidad de dispositivos recopilan, almacenan, procesan y comparten información. La seguridad del sistema está amenazada por problemas que afectan a...

- **Confidencialidad**
  - La información permanece accesible solo a quien esté **autorizado**
- **Integridad**
  - Modificaciones no **autorizadas** de la información no pasan desapercibidas
- **Disponibilidad**
  - El sistema ofrece su servicio cuando un usuario **autorizado** lo solicita

1. Identificación

En todo sistema existe un "usuario virtual" que representa los privilegios de un "usuario real". Solo dicho usuario real podrá ostentar los poderes de su usuario virtual.

En el proceso de identificación, el usuario real "reclama" los poderes de un usuario virtual.

Tras la identificación, el sistema debe verificar que el usuario virtual efectivamente representa los privilegios del usuario real que los reclama

> Identificación $\rightarrow$ Verificación $\rightarrow$ Autorización

Identificación/Verificación

El mecanismo clásico es el de la pareja usuario/contraseña

- Punto vulnerable si el atacante accede a la lista de contraseñas
  - Por ello se suele guardar solo un hash de la contraseña
- Susceptible a ataques de diccionario
- Existen mecanismos de fortalecimiento de las contraseñas
  - Incorporación de bits aleatorios (sal) junto a la contraseña como entrada al hash
  - Contraseñas de un solo uso Pn= f(Pn−1)
- Existen diversos protocolos de autentificación que trabajan con contraseñas (Ej. Radius y Kerberos)

Otros mecanismos para la identificación-verificación son claves hardware y tarjetas inteligentes; o parámetros biométricos como huella dactilar, retina, iris, voz, cara...

2. Confidencialidad

La confidencialidad se garantiza si la información permanece accesible solo a quienes están autorizados

> $A \rightarrow m \rightarrow B$

Si C se encarga de velar por la seguridad ¿Debería poder ver el mensaje m?

Mecanismos de confidencialidad

- Cifrado de mensajes
  - Principal mecanismo de protección de confidencialidad
  - Ya usado por el emperador romano Julio Cesar
  - Se debe parametrizar el algoritmo de cifrado y maximizar la privacidad de los parámetros usados (claves)
    - ¿Nos beneficia ocultar el algoritmo de cifrado? AES (Advanced Encryption Standard, uno de los algoritmos de cifrado más utilizados y seguros actualmente) fue elegido entre 15 candidatos que fueron puestos a prueba, es de acceso público.

      En general, si el algoritmo es público damos banda a que la gente ponga a prueba el algoritmo, permitiendo que los puntos flacos sean detectados rápidamente por la comunidad y se corrijan. Si lo mantenemos privado, cuando se descubran esos puntos débiles (*when, not if*), se explotarán y no sabremos de dónde proviene la debilidad así que se tardará más en subsanarlos.
  - Algunas opciones de cifrado de mensajes:
    - Cifrado de bloque - Ej. AES
    - Cifrado de flujo - Ej. RC4
    - Cifrado simétrico - Ej. DES
    - Cifrado asimétrico - Ej. RSA
    - Cifrado híbrido - Ej. PGP

Vulnerabilidades

La seguridad de un sistema de cifrado no debe recaer en la ocultación del algoritmo de cifrado sino en un espacio de claves suficientemente grande y una gestión adecuada de las claves

¿Cuáles son las vulnerabilidades de un sistema de cifrado? Los elementos susceptibles de presentar problemas son:

- Algoritmo
- Implementación del algoritmo
- Gestión de claves

Las vulnerabilidades habituales son:

- Errores en los protocolos
- Gestión incorrecta de claves
- Defectos de implementación
- Vulnerabilidades físicas

3. Integridad

Garantía de que las modificaciones no autorizadas de la información no pasarán desapercibidas. No se trata de evitar que se modifique la información, sino de detectar si ha sido modificada

Mecanismos

Para garantizar la integridad tenemos varias alternativas:

- **HASH**: para fortalecer la integridad se añade a los mensajes información redundante que ayuda a detectar modificaciones.
    - MD5, SHA-1, Tiger, Whirpool

  Un atacante podría modificar el mensaje y componer un nuevo código hash. El receptor no podrá advertir que el mensaje fue alterado.
- **Códigos de autentificación de mensaje (MAC)**: códigos de detección de modificación parametrizados mediante una clave secreta.

  El atacante no puede modificar el mensaje sin ser detectado, puesto que no conoce la clave usada en la generación del código detector. Para poder verficar la integridad, el receptor necesita conocer la clave.
- **Firma digital**: protocolo de clave pública/privada.
    - La clave privada se emplea para generar la firma que permite detectar modificaciones.
    - La clave pública pertite verificar la integridad y autoría del mensaje.

  Es recomendable separar las claves de cifrado de las claves de firma.

	¿Quién genera el código de detección?	**¿Quién lo verifica?**
HASH	Cualquiera, el algoritmo es público	Cualquiera, el algoritmo es público
MAC	Quien posea la clave	Quien posea la clave
Firma digital	Quien posea la clave	Cualquiera, el algoritmo y clave son públicos

1. Si **A** envía un mensaje **m** a **B** ¿Puede **B** convencer a **C** de que el mensaje es legítimo?
2. Si todos conocen la clave ¿Puede C confiar en que B no modificó el mensaje original?

Condición de no repudio

Garantía de la integridad y autoría de un mensaje

Pregunta en PRADO: La condición de integridad garantiza...

> 1. ...que el mensaje no fue modificado -- FALSO, es imposible garantizarlo
> 2. ...que el mensaje no fue modificado por un usuario no autorizado -- FALSO, es imposible garantizarlo
> 3. ...que el mensaje no fue modificado por un usuario no autorizado sin que el receptor se percate de dicha modificación -- VERDADERO
> 4. ...que el mensaje solo puede ser leído por un usuario autorizado -- FALSO, nada que ver
>
> RESPUESTA: 3

4. Disponibilidad

Garantía de que el sistema ofrece su servicio a un usuario autorizado cuando lo solicita. Cuando el sistema no es capaz de atender los servicios solicitados, se encuentra en una condición de **denegación de servicio** (DoS)

La condición de denegación de servicio se puede producir por:

- **Ataque al canal de comunicación:** los usuarios legítimos compiten con el atacante por el uso de un recurso limitado: el canal de comunicación.
    - ¿Cómo prevenir ataques al canal de comunicación?
        - **Técnicas de comunicación encubierta**
            - Emisión por canales cambiantes en función de una función pseudoaleatoria conocida por emisor y receptor. Válidas cuando se establece comunicación con clientes conocidos.
        - **Control de acceso plutocrático**
            - El cliente paga por uso del servicio
            - Se puede establecer un precio no uniforme
        - **Protocolo de puzzle**
            - El sistema ofrece al cliente una prueba que le requerirá cierto poder computacional para resolverla
            - Esto previene el saturar los recursos del sistema pero no previene los problemas de ataque al canal
- **Ataque a las baterías (tortura por privación de sueño):**
    - ¿Cómo prevenir tortura por privación de sueño?
        - Establecimiento de una reserva de recursos para usuarios legítimos
        - Establecimiento de cuota de uso

Pregunta en PRADO: El panel de información del recibidor de la ETSIIT ajusta su funcionamiento para ofrecer información a quien la solicite (aunque no sean ni trabajadores del centro ni estudiantes) y por ello es necesario garantizar su disponibilidad. ¿Qué técnica podemos usar para garantizarla?

> 1. Técnicas de comunicación encubierta para prevenir el agotamiento de las baterías -- FALSO, comunicación encubierta no tiene nada que ver con las baterías
> 2. Control de acceso plutocrático -- FALSO, la información es para quien la solicite, aunque no sea estudiante (es decir, no pague)
> 3. Técnicas de comunicación encubierta para prevenir ataques al canal de comunicaciones -- FALSO, aunque sí tiene que ver con el canal de comunicaciones, no es adecuado porque no conocemos los clientes que acceden
> 4. Todas las anteriores opciones son falsas -- VERDADERO
>
> RESPUESTA: 4. En este caso, usaríamos el protocolo de puzzle