IIC2523
Sistemas Distribuidos

Hernán F. Valdivieso López
(2025 - 2 / Clase 18)

Introducción a ataques y seguridad a una red
¿Cómo está comprometida nuestra seguridad?

Temas de la clase

1. Ataque a un sistema
    a. Modelo "Enemigo"
    b. Tipos de amenazas
    c. Métodos de ataque
2. Medidas de Seguridad

Ataque a un sistema

Modelo "Enemigo"

Tipos de amenazas

Métodos de ataque

Ataque a un sistema

- En sistemas distribuidos, comprender las amenazas y ataques es fundamental para diseñar sistemas seguros y confiables.
- Los ataques a un sistema buscan comprometer alguno de los tres pilares de la seguridad.
  - **Confidencialidad** → Garantiza que no se divulgue la información privada.
  - **Integridad** → Garantiza que los datos se envían y almacenan correctamente.
  - **Disponibilidad** → Garantiza que el sistema esté disponible cuando corresponda.

Ataque a un sistema - Modelo Enemigo

- Para analizar las amenazas de seguridad, a menudo se postula un enemigo (también conocido como adversario).
- Este enemigo es un modelo conceptual que representa a un atacante con ciertas capacidades:
  - Es capaz de enviar cualquier mensaje a cualquier proceso.
  - Puede leer o copiar cualquier mensaje enviado entre un par de procesos.
  - Puede generar mensajes con una dirección de origen falsificada.
  - Sus ataques pueden provenir de una computadora legítimamente conectada a la red o de una conectada de manera no autorizada.
- Asumir un enemigo con estas capacidades nos permite anticiparnos y diseñar medidas de seguridad más potentes.

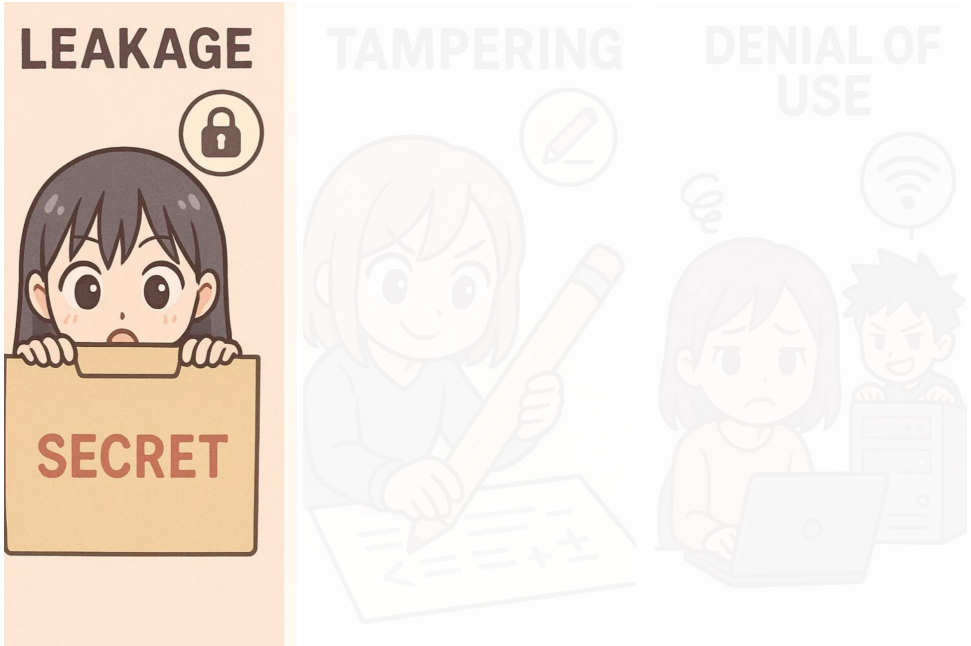
Ataque a un sistema - Tipos de Amenazas

- Las amenazas a la seguridad de los sistemas informáticos se dividen en tres clases principales.

- ***Leakage* - Fuga de información**

  Adquisición de información por parte de receptores no autorizados.

  Esto también puede ocurrir de formas sutiles, como inferir información a partir de la mera existencia de un mensaje o del patrón de tráfico.



Fuente: OpenAI. (2025). [Representación de tipos de amenazas] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Ataque a un sistema - Tipos de Amenazas

- Las amenazas a la seguridad de los sistemas informáticos se dividen en tres clases principales.

- ***Tampering*** **- Manipulación de información**

  Alteración no autorizada de la información.

  Puede ir desde modificar contenido para afectar la seguridad del sistema o para impedir que el usuario haga la solicitud correctamente.

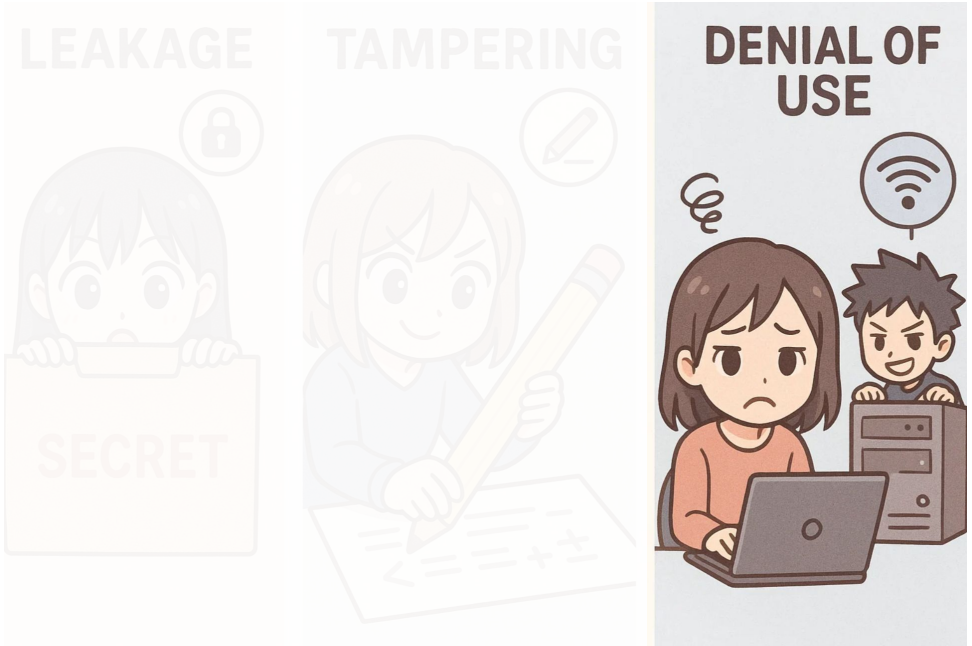
Fuente: OpenAI. (2025). [Representación de tipos de amenazas] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Ataque a un sistema - Tipos de Amenazas

- Las amenazas a la seguridad de los sistemas informáticos se dividen en tres clases principales.

- ***Denial of Use* - denegación de uso**

  Se refiere a la interferencia con el funcionamiento adecuado de un sistema sin que el perpetrador obtenga un beneficio directo. Esto se manifiesta típicamente como ataques de denegación de servicio.



Fuente: OpenAI. (2025). [Representación de tipos de amenazas] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Ataque a un sistema - Tipos de Amenazas (Resumen)

- Un sistema de información debe tener preocupación de estas 3 posibles amenazas que puede sufrir a partir de distintos tipos de ataques
  - Fuga de información
  - Manipulación de información
  - Negación a la información

Ataque a un sistema - Métodos de ataque

- Los ataques en sistemas distribuidos explotan canales de comunicación legítimos o simulan conexiones autorizadas para obtener acceso.
- Algunos ejemplos de ataques son:
  - *Eavesdropping*
  - *Masquerading*
  - *Message Tampering*
  - *Distributed Denial of Service - DDoS*

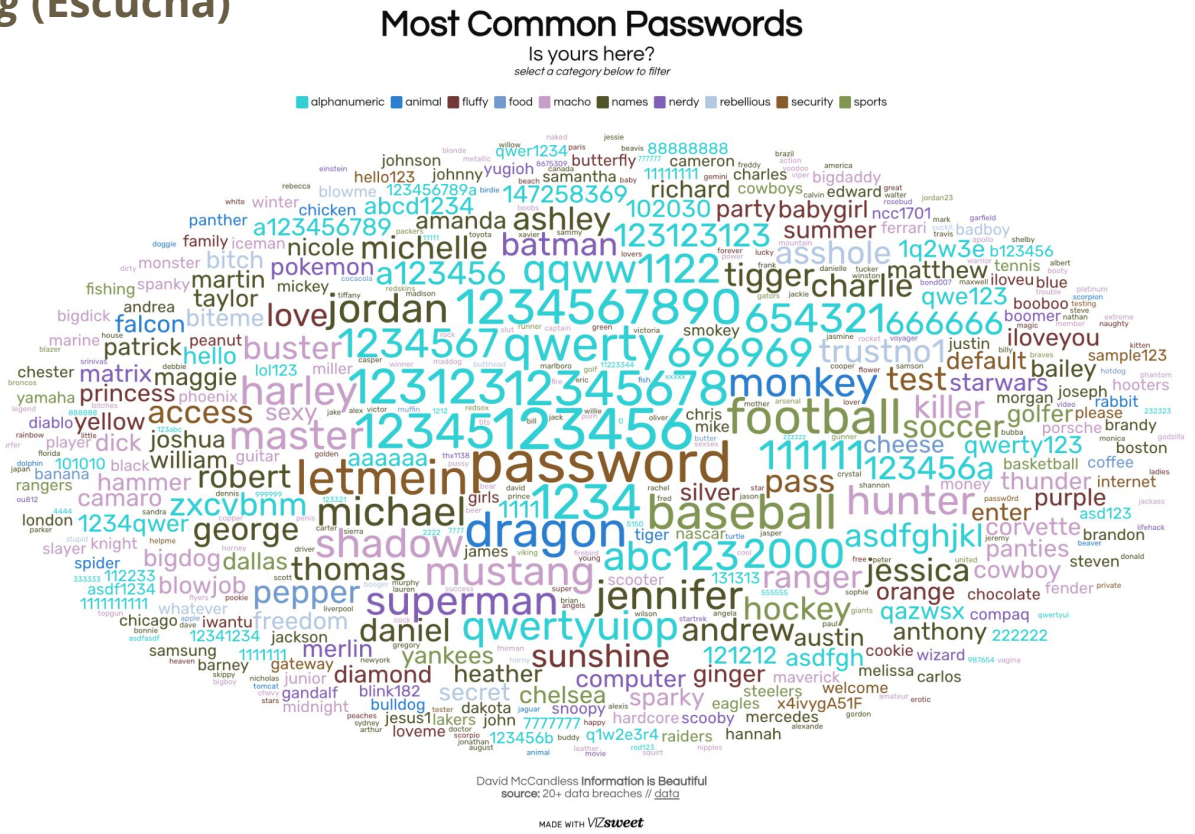
Ataque a un sistema - Métodos de ataque

***Eavesdropping* (Escucha)**

- Consiste en obtener copias de mensajes sin autorización.
- Por ejemplo, en la mayoría de las redes locales, es fácil ejecutar un programa para obtener copias de mensajes transmitidos entre otras computadoras.
- Diez años después de las filtraciones de Snowden, más datos y más controles - SWI swissinfo.ch
- 16 billion passwords exposed in colossal data breach | Cybernews

Ataque a un sistema - Métodos de ataque

Eavesdropping (Escucha)



Fuente: [Top 500 Most Common Passwords Visualized Is yours here?]

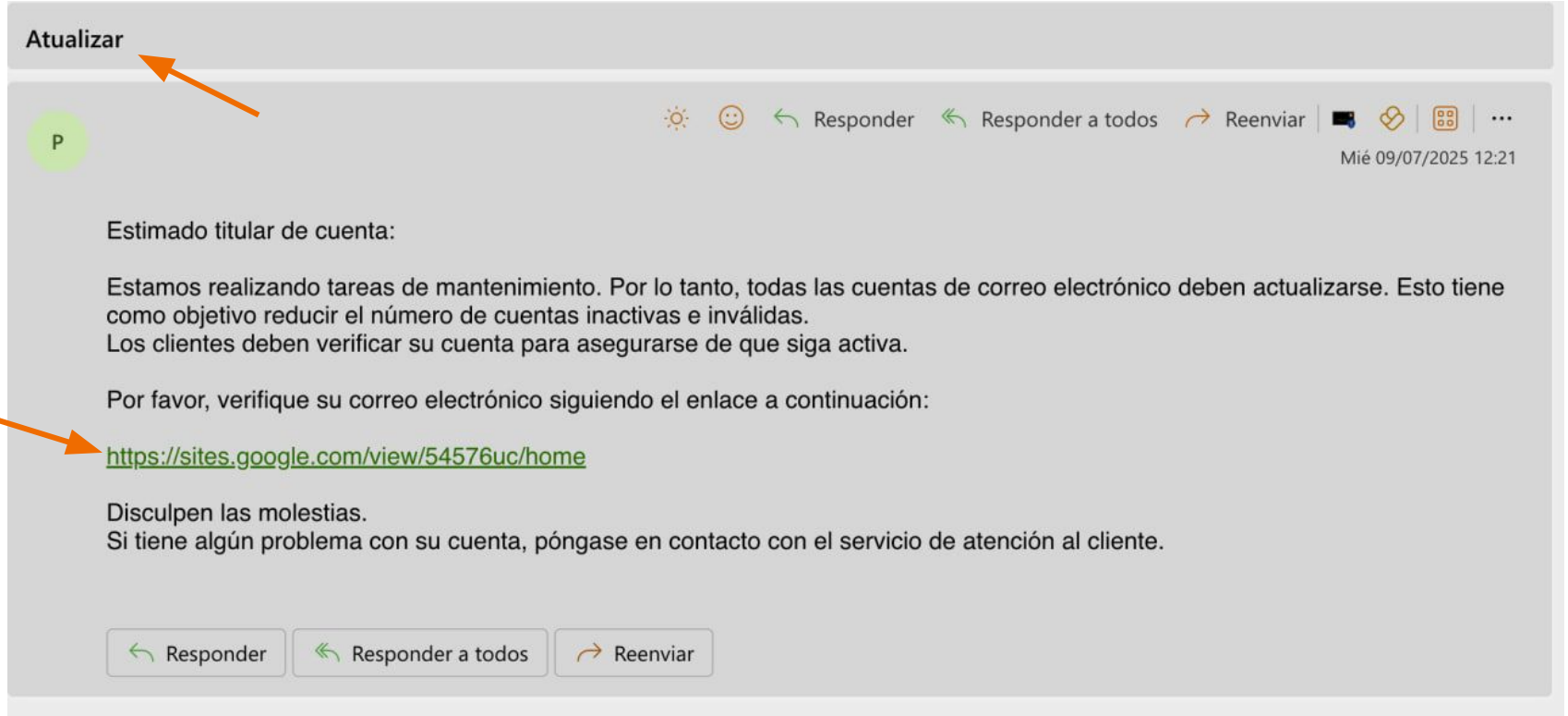
Ataque a un sistema - Métodos de ataque

***Masquerading* (Suplantación de identidad)**

- Implica enviar o recibir mensajes utilizando la identidad de otro principal (persona, *software* o dispositivo) sin su autoridad.
- El *phishing* es una tipo de ataque para lograr obtener información confidencial del usuario y luego usarla para suplantar su identidad.
  - Obtener contraseñas.
  - Datos de la tarjeta de crédito/débito.
- Hong Kongers lose B870m to scams in a week, AI voice-cloning used
- PDI alerta de nueva estafa: Clonan voces de personas con inteligencia artificial para engañar - Cooperativa.cl

Ataque a un sistema - Métodos de ataque

Masquerading (Suplantación de identidad)



Ataque a un sistema - Métodos de ataque

***Message Tampering* (Manipulación del mensaje)**

- Alteración no autorizada de un mensaje para cambiar su significado o intención original.
- Ataques "*Man-in-the-Middle*", Manipulación de parámetros web (inyección SQL) o manipulación de código fuente.
- Is Stuxnet the 'best' malware ever?
  - Modifica instrucciones del computador

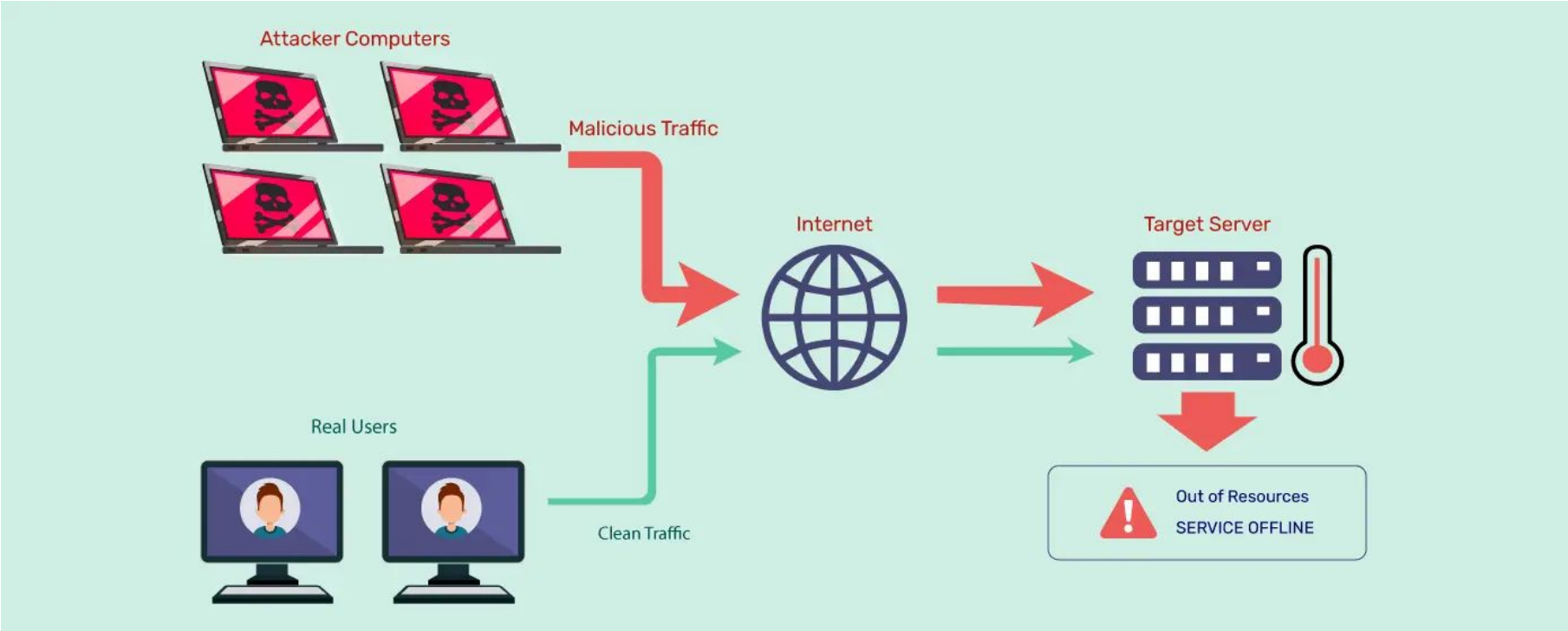
Ataque a un sistema - Métodos de ataque

***Distributed Denial of Service - DDoS* (Denegación de servicio)**

- Es una forma de ataque en la que el enemigo interfiere con las actividades de los usuarios autorizados mediante la realización de invocaciones excesivas y sin sentido a los servicios o transmisiones de mensajes en una red.
- *Distributed* es porque el ataque viene de muchas fuentes lo que lo hace más difícil de defender que un ataque de denegación de servicio.
- Busca una sobrecarga de los recursos físicos (ancho de banda de la red, capacidad de procesamiento del servidor).
- El objetivo suele ser retrasar o impedir acciones de otros usuarios.
- GitHub Survived the Biggest DDoS Attack Ever Recorded

Ataque a un sistema - Métodos de ataque

Denial of Service - DoS (Denegación de servicio)



Fuente: Ataques DDoS: ¿qué son y cómo se pueden evitar?

Ataque a un sistema - Métodos de ataque (Otros)

Existen muchos más tipos de ataques 🔪

- ***Sybil*:** se crean múltiples identidades falsas para manipular el comportamiento del sistema (por ejemplo, votaciones o reputación).
- ***Eclipse*:** se aísla a un nodo objetivo controlando todas sus conexiones de red, bloqueando su visión del sistema.
- ***Replay Attack*:** se interceptan y re-transmiten mensajes válidos para engañar al sistema, haciéndole creer que son recientes.
- ***Routing Attack*:** se manipula la información de enrutamiento (como en DHTs o P2P) para redirigir o interceptar datos.

Ataque a un sistema - Métodos de ataque (Otros)

Existen muchos más tipos de ataques 🔪

- ***Sybil*: se crean múltiples identidades falsas para manipular el comportamiento del sistema (por ejemplo, votaciones o reputación).
- ***Eclipse*: se aísla a un nodo objetivo controlando todas sus conexiones de red, bloqueando su visión del sistema.
- ***Replay Attack*: se interceptan y re-transmiten mensajes válidos para engañar al sistema, haciéndole creer que son recientes.
- ***Routing Attack*: se manipula la información de enrutamiento (como en DHTs o P2P) para redirigir o interceptar datos.

Estudiaremos algunos de estos con más profundidad en próximas clases 😁

Medidas de Seguridad

Medidas de Seguridad

- El diseño de sistemas seguros parte de una lista de amenazas y un conjunto de suposiciones de "peor caso".
  - Asumir que el adversario es un "*big-boss*" → inteligente y con mucho poder de ataque.
- Es necesario un análisis cuidadoso de las amenazas que puedan surgir de todas las fuentes posibles en el entorno de red, el entorno físico y el entorno humano del sistema.
- Lo más recomendado ee construir un modelo de amenazas que enumere todas las formas de ataque a las que el sistema está expuesto y una evaluación de los riesgos y consecuencias de cada una.

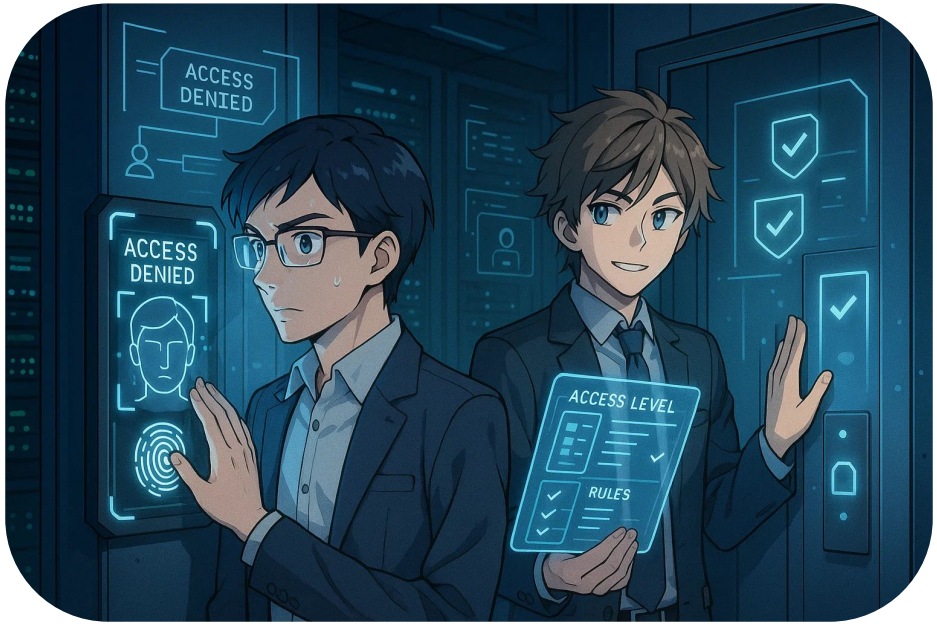
Medidas de Seguridad

- **Cifrado**: Oculta el contenido de los mensajes.
  - Intenta protegernos de ataques *Eavesdropping* y *Message Tampering*.

Fuente: OpenAI. (2025). [Representación de Cifrado] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Medidas de Seguridad

- **Autenticación y Autorización**: Verifica la identidad declarada de una entidad y asegura que solo puedan realizar operaciones para las que tienen permiso.
  - Intenta protegernos de ataques *Masquerading*.



Fuente: OpenAI. (2025). [Representación de Autenticación] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Medidas de Seguridad

- **Canales seguros**: Usan técnicas criptográficas y de autenticación para garantizar la privacidad y la integridad de los datos transmitidos.
  - Intenta protegernos de ataques *Eavesdropping*, *Message Tampering* y *Masquerading*.

Fuente: OpenAI. (2025). [Representación de canales seguros] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Medidas de Seguridad

- **Monitoreo**: Rastrean los accesos a los activos del sistema para detectar intrusiones no autorizadas externos o internas.
  - Intenta protegernos de ataques *Denial of Service - DoS* o de ataques internos.

Fuente: OpenAI. (2025). [Representación de monitoreo] [Imagen generada por inteligencia artificial con Sora]. https://openai.com/sora

Medidas de Seguridad

- En las siguientes clases abordaremos diferentes técnicas utilizadas por los sistemas para defenderse de los ataques
  - Cifrado
  - Autorización y autenticación
  - Canales seguros
  - Monitoreo

Medidas de Seguridad - Debate

- Equilibrio entre Seguridad y otras propiedades.
- El diseño de sistemas distribuidos seguros y privados implica a menudo compensaciones difíciles.
- ¿Cuáles *trade-off* se les ocurre que pueden existir?

Medidas de Seguridad - Debate

- Equilibrio entre Seguridad y otras propiedades.
- El diseño de sistemas distribuidos seguros y privados implica a menudo compensaciones difíciles.
- ¿Cuáles *trade-off* se les ocurre que pueden existir?
  - **Rendimiento vs Seguridad** → La criptografía tiende a ser costosa.

Medidas de Seguridad - Debate

- Equilibrio entre Seguridad y otras propiedades.
- El diseño de sistemas distribuidos seguros y privados implica a menudo compensaciones difíciles.
- ¿Cuáles *trade-off* se les ocurre que pueden existir?
  - **Rendimiento vs Seguridad** → La criptografía tiende a ser costosa.
  - **Usabilidad vs Seguridad** → Tantos mecanismos de autenticación (2 fases, *login* periódicos) afecta a la usabilidad del sistema.

Medidas de Seguridad - Debate

- Equilibrio entre Seguridad y otras propiedades.
- El diseño de sistemas distribuidos seguros y privados implica a menudo compensaciones difíciles.
- ¿Cuáles *trade-off* se les ocurre que pueden existir?
  - **Rendimiento vs Seguridad** → La criptografía tiende a ser costosa.
  - **Usabilidad vs Seguridad** → Tantos mecanismos de autenticación (2 fases, *login* periódicos) afecta a la usabilidad del sistema.
  - **Privacidad vs Seguridad** → Rastrear todas las acciones del usuario puede ser una invasión a su privacidad.

Medidas de Seguridad - Debate

- Equilibrio entre Seguridad y otras propiedades.
- El diseño de sistemas distribuidos seguros y privados implica a menudo compensaciones difíciles.
- ¿Cuáles *trade-off* se les ocurre que pueden existir?
  - **Rendimiento vs Seguridad** → La criptografía tiende a ser costosa.
  - **Usabilidad vs Seguridad** → Tantos mecanismos de autenticación (2 fases, *login* periódicos) afecta a la usabilidad del sistema.
  - **Privacidad vs Seguridad** → Rastrear todas las acciones del usuario puede ser una invasión a su privacidad.
- 🤔 ¿Qué prefieren ustedes? ¿Para qué caso es mejor uno que otro? 🤔

Poniendo a prueba lo que hemos aprendido 👀

¿Cuál de las siguientes afirmaciones es **correcta** respecto a los ataques y amenazas en sistemas distribuidos?

a. El cifrado impide que un atacante pueda interceptar los mensajes en tránsito.

b. La suplantación de identidad solo ocurre cuando se manipula el contenido del mensaje.

c. El modelo del enemigo considera que puede leer, falsificar y manipular mensajes transmitidos entre procesos.

d. El modelo del enemigo supone que este solo puede atacar desde fuera de la red.

e. Un ataque de denegación de servicio busca obtener acceso no autorizado a datos confidenciales.

Poniendo a prueba lo que hemos aprendido 👀

¿Cuál de las siguientes afirmaciones es **correcta** respecto a los ataques y amenazas en sistemas distribuidos?

a. El cifrado impide que un atacante pueda interceptar los mensajes en tránsito.

b. La suplantación de identidad solo ocurre cuando se manipula el contenido del mensaje.

c. El modelo del enemigo considera que puede leer, falsificar y manipular mensajes transmitidos entre procesos.

d. El modelo del enemigo supone que este solo puede atacar desde fuera de la red.

e. Un ataque de denegación de servicio busca obtener acceso no autorizado a datos confidenciales.

Próximos eventos

Próxima clase

- Última materia que entra en la I2: Cifrado de mensajes
- ¿Qué métodos existen para proteger un mensaje?

Evaluación

- Estamos con Tarea 3, se entrega este domingo.
- El control 5 se publica el miércoles, se entrega el otro miércoles a las 20:00. La clase del 22 de octubre la dedicaremos exclusivamente para trabajar en el control.

IIC2523
Sistemas Distribuidos

Hernán F. Valdivieso López
(2025 - 2 / Clase 18)