



# INICIO GRABACIÓN



**SANJOSÉ**  
FUNDACIÓN DE EDUCACIÓN SUPERIOR

The background features a photograph of two hands shaking in a firm grip, symbolizing agreement or partnership. This image is partially covered by two overlapping circles: a light blue one on the left and a dark blue one on the right. The text is centered within the intersection of these circles.

# SEGURIDAD EN LOS SISTEMAS DISTRIBUIDOS



# SEGURIDAD EN UN SISTEMA DISTRIBUIDO




## ***1. ¿Cuales son las amenazas y Ataques que hay en los sistemas distribuidos?***

En la mayoría de los tipos de redes locales es fácil construir un programa sobre un computador conectado para que obtenga copias de los mensajes transmitidos entre computadores. Otras amenazas son mas sutiles; un programa podría situarse a si mismo en lugar del autentico servidor de archivos y así obtener copias de información confidencial que los clientes, inconscientemente, envían para su almacenamiento.

Además del peligro de daño de información pueden aparecer reclamaciones fraudulentas contra el propietario de un sistema que no sea demostrablemente seguro. Para evitarlo, el propietario debe desacreditar la reclamación mostrando que el sistema es seguro contra tales violaciones, o produciendo un registro histórico de todas las transacciones. Un ejemplo es el *débito fantasma* en los cajeros automáticos. La mejor respuesta de un banco es proporcionar un registro de la transacción firmado digitalmente por el titular de la cuenta, que no pueda ser falsificado.

La principal meta de la seguridad es restringir el acceso a la información y los recursos de modo que solo tengan acceso aquellos que estén autorizados.





Las amenazas de seguridad se dividen en tres clases:

**Fuga:** la adquisición de información por receptores no autorizados.

**Alteración:** la modificación no autorizada de información.

**Vandalismo:** interferencia en el modo de operación adecuado de un sistema, sin ganancia para el responsable. Los ataques en los sistemas distribuidos dependen de la obtención de acceso a los canales de comunicación. Los métodos de ataque pueden clasificarse en función del modo en que se abusa del canal:

**Fisgar :** obtener copias sin autorización.

**Suplantar:** enviar o recibir mensajes utilizando la identidad de otro sin su autorización.

**Alterar mensajes** — interceptar mensajes y alterar sus contenidos antes de pasarlos al receptor.

**Reenviar:** almacenar mensajes interceptados y enviarlos mas tarde.

**Denegación de servicio:** desbordar un canal o recurso para impedir que otros accedan a el. Los ataques victoriosos dependen del descubrimiento de agujeros en la seguridad de los sistemas y estos problemas son comunes en los sistemas de hoy.

Cuando se diseño Internet y los sistemas conectados a ella, la seguridad no era una priorizadla incorporación de medidas de seguridad requiere ser cuidadoso con la etapa de diseño.

Nos hemos concentrado en los ataques a los sistemas distribuidos que nacen de la exposición de sus canales de comunicación y sus interfaces. Los mecanismos de seguridad no pueden protegernos contra una clave de acceso mal elegida o custodiada. Pero para sistemas que incluyan programas móviles y sistemas cuya seguridad sea sensible a la fuga de información, hay mas ataques.



# SEGURIDAD EN UN SISTEMA DISTRIBUIDO

**Fugas de Información:** Si pudiera observarse la sucesión de mensajes en la comunicación entre dos procesos, sería posible vislumbrar información importante aun de su sola existencia. Hay muchas formas sutiles de fugas de información, algunas maliciosas y otras que son consecuencia de errores inadvertidos. El potencial de las fugas aparece cuando se pueden observar los resultados de un computo. La aproximación empleada es la asignación de niveles de seguridad a la información y los canales, y analizar el flujo de información hacia los canales con el objetivo de asegurar que la información de alto nivel no fluya hacia los canales de bajo nivel.

## ***2.¿En que consiste la Seguridad de las Transacciones Electrónicas?***

Muchas aplicaciones de comercio y demás implican transacciones que dependen de la seguridad, como ser:

- E-mail: hay muchos usos del correo en que los mensajes deben ser confidenciales (como enviar un numero de tarjeta de crédito).
- Compra de bienes y servicios: estas transacciones son usuales. Los compradores seleccionan bienes y pagan por ellos empleando el Web, luego le son enviados por un mecanismo de reparto.

Transacciones bancarias: los bancos electrónicos ofrecen a los usuarios todos los servicios que proporcionan los bancos convencionales.

- Micro-transacciones: Internet se presta a proporcionar pequeñas cantidades de información y otros servicios hacia sus clientes. Por ejemplo, el acceso a la mayoría de las paginas Web no exige ningún pago, pero el desarrollo del Web como un medio de publicación de alta calidad seguramente depende de hasta que punto los proveedores de información puedan obtener beneficio de los clientes de esta información.

Las transacciones como estas solo se pueden realizar de modo seguro cuando se encuentran protegidas contra la revelación de los códigos de crédito durante la transmisión, y contra un vendedor fraudulento que obtenga un pago sin intención de proveer bien alguno.



# SEGURIDAD EN UN SISTEMA DISTRIBUIDO




## 3. Cuales son los requisitos que exige?

Una política de seguridad sensata para vendedores y compradores de Internet exige los siguientes requisitos:

- Autenticación del vendedor al comprador.
- Mantenimiento del numero de tarjeta de crédito y otros detalles del comprador bajo secreto, y asegurar que se transmiten de forma inalterada del comprador al vendedor.
- Si los bienes se encuentran en una forma útil para su descarga, asegurar que su contenido llega al comprador sin alteración y sin ser desvelados a terceras partes.

Las necesidades de seguridad de las transacciones bancarias que emplean una red abierta son similares a las de las transacciones de compra, con el titular de la cuenta y el banco como vendedor, aunque hay necesidad de:

- Autenticar la identidad del titular de la cuenta hacia el banco antes de darle acceso a su cuenta.
  - En esta situación es importante para el banco estar seguro de que el titular de la cuenta no pueda negar haber participado en una transacción. A esto se le da el nombre de no repudio.
  - El comercio en Internet es una aplicación importante de las técnicas de seguridad, pero no es ciertamente la única. Es una necesidad cuando quiera que dos computadores sean utilizados por individuos u organizaciones para almacenar y comunicar información importante.
- 





#### 4. ¿En que consiste el Diseño de Sistemas Seguros?

Debemos diferenciar las tareas específicas de un diseñador de sistemas seguros y de un programador. El objetivo del diseñador es excluir todos los posibles ataques y agujeros. La situación es análoga a la del programador cuyo principal objetivo es excluir todos los errores de su programa. En ningún caso existe un método concreto para asegurar las metas durante el diseño. Cada uno diseña con los mejores estándares disponibles y aplica un análisis informal y comprobaciones. Una vez que un diseño está completo, una opción es la validación formal. La seguridad trata de evitar los desastres y minimizar los contratiempos. Cuando se diseña para seguridad es necesario pensar siempre en lo peor.

Para demostrar la validez de los mecanismos de seguridad, empleados en un sistema, los diseñadores deben construir, en primer lugar, una lista de amenazas y probar que cada una de ellas se puede prevenir mediante los mecanismos empleados como por ej. Un histórico de seguridad. Un histórico de seguridad contendrá una secuencia de registros fechados de las acciones de los usuarios. Como mínimo, los registros incluirán la identidad del principal, la operación realizada), la identidad del objeto sobre el que se opera y la fecha y hora.

Donde se sospeche que pudiera haber violaciones concretas, los registros pueden contener información a mayores para incluir la utilización de los recursos físicos (ancho de banda de red, periféricos), o disparar un procedimiento histórico especial de operaciones sobre objetos concretos. Posteriormente se puede efectuar un análisis de carácter estadístico o bien basado en búsquedas. Incluso aunque no se sospeche de alguna violación, las técnicas estadísticas permitirán comparar registros a lo largo del tiempo para descubrir tendencias o cualquier suceso inusual.

El diseño de sistemas seguros es un ejercicio de balance entre los costos y las Amenazas ya que:

- Su uso acarrea un costo (en esfuerzo computacional y uso de la red). Los costos deben compensar la amenaza.
- Unas especificaciones de medidas de seguridad inapropiadas podrían impedir a los usuarios legítimos el realizar ciertas acciones necesarias.



## 5. ¿Qué significa “Problema de Seguridad”?

- Aquellos que comprometen la integridad o la privacidad de los datos almacenados.
- Aquellos que permiten acceso a recursos supuestamente no permitidos.
- Aquellos que impiden el acceso a recursos a usuarios legítimos.
- Aquellos que permiten hacer un mal uso de los recursos informáticos.

## 6. ¿Los sistemas son seguros?

Virus informáticos, Troyanos, Gusanos.

- Páginas Web “hostiles”.
- “Spyware”.
- Entradas en sistemas ajenos.
- Robo de datos bancarios.
- Cambio de páginas Web.
- Ataques Dos a nivel mundial.

## 7. Razones de la inseguridad?

### 1. En Internet:

- Origen de Internet: Abierta, cooperativa.
- Web: Acceso masivo a personas sin conocimientos. (deseable, pero peligroso)
- Nodos no administrados.
- Las mismas que la inseguridad en ordenadores

### 2. En redes:

Instalaciones “por defecto” no pensadas para la seguridad.

- Facilitar al máximo todo al usuario, automatización. Seguridad vs. Comodidad.
- Complejidad de los sistemas, interacciones no previstas.
- Sistemas “distribuidos”
- Desconocimiento en temas de seguridad por parte de los programadores.



The background of the slide features a photograph of two hands shaking, symbolizing agreement or partnership. This image is partially covered by a large, semi-transparent blue circle. Inside this circle, the title text is displayed in white, bold, uppercase letters. A small, solid blue sphere is located at the bottom right of the large blue circle.

# MODELOS EN LOS SISTEMAS DISTRIBUIDOS

# Diseño de Arquitecturas Distribuidas



## Calidad de Servicio

Propiedades no funcionales: *fiabilidad *seguridad *prestaciones	La facilidad de adaptación para adecuar configuraciones variables de sistema y disponibilidad.	Algunas aplicaciones mantienen datos críticos en el tiempo, flujos de datos que precisan ser procesados o transferidos de un proceso a otro	Implica un requisito para que el sistema proporcione recursos garantizados de computación y comunicación que sean suficientes para permitir a las aplicaciones finalizar cada tarea a tiempo	Cada recurso crítico debe reservarse para las aplicaciones que requieren QoS y deben ser los gestores de los recursos los que proporcionen las garantías. Las solicitudes de reserva se pueden
---	--	---	--	---



# Modelos Fundamentales en un Sistema Distribuido

Todas las arquitecturas comparten algunas propiedades fundamentales:

Procesos que se comunican por paso de mensajes a través de una red de computadores . En particular, trataremos con tres aspectos

- \* **Interacción:** el modelo debe definir y clasificar la comunicación entre elementos del sistema
- \* **Fallos:** el modelo debe definir y clasificar los fallos que pueden darse en el sistema.
- \* **Seguridad:** el modelo debe definir y clasificar los tipos de ataque que pueden afectar al sistema.



# Modelos de Interacción

1. **Respecto a la interacción**, los sistemas distribuidos deben tener en cuenta que :

- \* Hay limitaciones debidas a la comunicación
- \* Es imposible predecir el retraso con el que llega un mensaje
- \* Es imposible tener una noción global de tiempo
- \* La ejecución es no determinista y difícil de depurar

2. **Algoritmo distribuido**

- \* Definición de los pasos que hay que llevar a cabo por cada uno de los procesos del sistema, *incluyendo los mensajes de transmisión entre ellos*



# Modelos de Interacción

## Prestaciones del canal de comunicación

### Latencia

- \* Retardo entre el envío de un mensaje y su recepción
- \* Ancho de banda
- \* Información que puede transmitirse en un intervalo de tiempo
- \* Fluctuación (jitter)  
Variación del tiempo invertido en repartir una serie de mensajes



# Modelos de Interacción

## Relojes y Eventos de tiempo

Cada computador tiene su propio reloj interno (reloj local)

- \* Puede usarse en procesos locales para marcas de tiempo
- \* Tasa de deriva de reloj (clock drift rate)
- \* Diferencia entre un reloj local y un reloj de referencia “perfecto”
- \* Receptores GPS
- \* Network Time Protocol (NTP)
- \* Mecanismos de ordenación de eventos
- \* Dos tipos de modelo de interacción
- \* Síncrono y asíncrono



# Modelos de Interacción

## Relojes y Eventos de tiempo

1. Cada computador tiene su propio reloj interno (reloj local)

- \* Puede usarse en procesos locales para marcas de tiempo

2. Tasa de deriva de reloj (clock drift rate)

- \* Diferencia entre un reloj local y un reloj de referencia “perfecto”

- \* Receptores GPS

- \* Network Time Protocol (NTP)

- \* Mecanismos de ordenación de eventos

3. Dos tipos de modelo de interacción

- \* Síncrono y asíncrono





# Modelos de Interacción



## Modelos síncronos

- \* Conocimiento de características temporales:
- \* El tiempo de ejecución de cada etapa de un proceso tiene ciertos límites inferior y superior conocidos.
- \* Cada mensaje transmitido sobre un canal se recibe en un tiempo límite conocido.
- \* Cada proceso tiene un reloj local cuya tasa de deriva sobre el tiempo de referencia tiene un límite conocido.
- \* A nivel teórico, podemos establecer unos límites para tener una idea aproximada de cómo se comportará el sistema.

A nivel práctico, es imposible garantizar esos límites siempre aunque a veces se pueden utilizar, por ejemplo como *timeouts*






# Modelos de Interacción



## Modelos asíncronos

- \* No hay limitaciones en cuanto a velocidad de procesamiento.
  - \* Retardos en la transmisión de mensajes
  - \* Tasas de deriva de los relojes
  - \* Los sistemas distribuidos reales suelen ser asíncronos. Por ejemplo, Internet
  - \* Una solución válida para un sistema asíncrono lo es también para uno síncrono
- 

# Modelos de Interacción

## Ordenación de eventos

Podemos describir un sistema en términos de eventos, solucionando así la falta de precisión de los relojes.

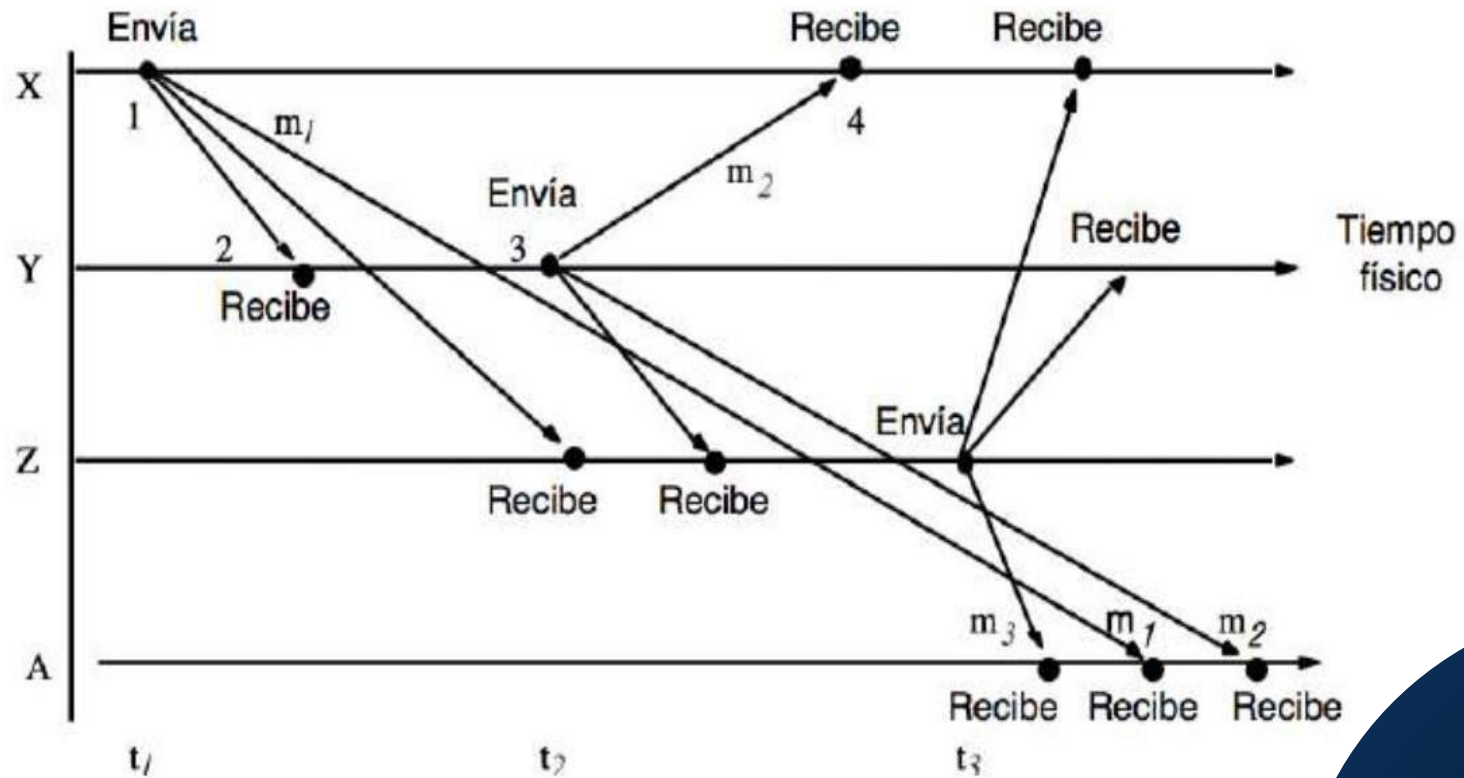
Imaginemos un grupo de usuarios de correo (X, Y, Z, A)

- \* X manda un mensaje  $m_1$  con el asunto *Reunión*
- \* Y y Z responden con mensajes  $m_2$  y  $m_3$ , respectivamente y en ese orden, con el asunto *Re:Reunión*
- \* Debido a la independencia en los retardos de cada envío, el usuario A podría ver lo siguiente:

Mensaje	De	Asunto
$m_3$	Z	Re: Reunión
$m_1$	X	Reunión
$m_2$	Y	Re: Reunión

# Modelos de Interacción

## Ordenación de eventos





# Modelos de Interacción

## Ordenación de Eventos

Si los relojes de X, Y y Z estuvieran sincronizados, podríamos incluir el tiempo local  $t_1$ ,  $t_2$ ,  $t_3$  en los mensajes  $m_1$ ,  $m_2$ ,  $m_3$

- \* Estaríamos seguros de que  $t_1 < t_2 < t_3$
- \* Podríamos ordenar los mensajes en concordancia
- \* Pero los relojes no suelen estar sincronizados
- \* Lamport [1978] propuso un modelo de tiempo lógico infiere el orden de los mensajes sin recurrir al tiempo físico.

Se basa en las siguientes afirmaciones

Un mensaje siempre se recibe después de enviarlo.

- *X manda  $m_1$  antes de que Y reciba  $m_1$*

La réplica no se envía hasta que no se ha recibido el original.

- *Y recibe  $m_1$  antes de que envíe  $m_2$*



# Modelos de Interacción

## Modelo de Fallo

Estudio de las causas posibles de fallo

- \* Para poder comprender sus consecuencias

Tipo de fallo según la entidad

- \* Fallos de proceso
- \* Fallos de comunicación

Tipo de fallo según el problema

- \* Fallos por omisión
- \* No se consigue realizar una acción que se debería poder hacer

Fallos arbitrarios (bizantinos)

- \* Errores de cualquier tipo, fuera del esquema de mensajes

Fallos de temporización

- \* Superación de tiempos límite en un sistema síncrono



# Modelos de Interacción

## Modelo de Fallo

Fallo del procesamiento (*crash*)

Detección del fallo por timeouts (síncrono)

- \*Si el proceso no responde, consideramos que ha habido un fallo
- \* En sistemas asíncronos, nunca podemos estar seguros

Fallo-parada (fail-stop)

- \*Fallo de procesamiento que puede ser detectado con certeza por el resto de procesos





FUNDACIÓN DE EDUCACIÓN SUPERIOR

**SAN JOSÉ**

INSTITUCIÓN TECNOLÓGICA

FIN DE  
GRABACIÓN