SEGURIDAD EN LOS SISTEMAS DISTRIBUIDOS

¿Qué es Seguridad?

- Capacidad del sistema para proteger datos, servicios y recursos de usuarios no autorizados.
  El fin de la seguridad es garantizar la protección o estar libre de todo peligro y/o daño.

El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan **Mecanismos de Protección**.

Los SO proveen algunos mecanismos de protección e implementa ***políticas de seguridad***.

Las políticas definen *qué hay que hacer* (qué datos y recursos deben protegerse de quién; etc), y los mecanismos determinan *cómo hay que hacerlo.*

Se distinguen las políticas de los mecanismos porque las políticas pueden variar en el tiempo y de una organización a otra. Y los mecanismos, son flexibles, pueden usarse para implementar distintas políticas.

Por otro lado, el uso de redes de computadoras y de SD se justifica si las medidas de seguridad pueden ser adecuadamente soportadas por el sistema o la red.

PROBLEMAS DE SEGURIDAD EN REDES

El usuario de una red espera que se distribuyan sus mensajes; que sólo se repartan al destinatario correcto; que se evite la pérdida, modificación u observación de los mensajes en tránsito. Esencialmente estos requerimientos no son más que las características usuales integridad, privacidad y disponibilidad.

Algunas razones que incrementan los problemas de seguridad de una red:

1. Compartición. Hay muchos más usuarios que tienen acceso potencial a una red que a un sistema individual, con lo que es más sencillo que haya usuarios maliciosos o simplemente ignorantes. Aún peor, el acceso se consigue a varios sistemas, por lo que los controles de acceso a un sistema individual pueden no ser adecuados para redes.

2. Complejidad del sistema. Los SO son complicados, difíciles de asegurar y más difíciles de certificar. Una red formada por posiblemente dos o más SO distintos es necesariamente más compleja que un sistema individual. Los controles desarrollados para uno de los sistemas pueden no ser adecuados para el otro y viceversa.

3. Perímetro desconocido. La capacidad de expansión que tiene una red hace que sus fronteras sean bastante difusas. Un anfitrión puede ser nodo de 2 redes distintas, por lo que los usuarios de cada una de ellas podrán acceder a la otra. Esto facilita la labor de usuarios maliciosos. Además, cada anfitrión debería ser capaz de reaccionar ante la presencia de un nodo nuevo, lo que no siempre es posible.

4. Muchos puntos de ataque. En un sistema informático individual el propio control de acceso puede garantizar la privacidad de los datos en dicho procesador. En una red, si un usuario está utilizando datos almacenados en un disco remoto estos datos pasarán a lo largo de muchos nodos. Es posible que muchos de ellos estén mantenidos por administradores competentes que garanticen la seguridad de los tránsitos, pero uno solo administrado por alguien incompetente o malicioso pone en peligro la privacidad de todas las transacciones.

5. Ruta desconocida. Debido a la complejidad de las conexiones entre distintos nodos de una red, es posible que haya más de un camino para conectar dos anfitriones distintos. Puede ocurrir que los nodos de uno de los caminos sean seguros, mientras que los de otros no lo son. El usuario no tiene forma de saber qué ruta seguirá su transacción.

Estos problemas nos conducen a:

1. Privacidad. La gran cantidad de usuarios desconocidos que hay en una red hace más difícil controlar y confiar en la información.

2. Integridad de los datos. El riesgo de que los datos que circulan por la red estén corrompidos es mayor. La corrupción puede darse por: modificación, inserción, borrado, repetición y reordenación de las transmisiones.

3. Autenticidad. No es fácil asegurar que un usuario o anfitrión son auténticos. Un anfitrión no tiene por qué confiar en la autentificación realizada por otro anfitrión.

4. Canales ocultos. Las redes ofrecen la posibilidad de crear canales ocultos de transmisión debido a la gran de datos que se transmiten a lo largo de ellas. Así podemos esconder mensajes sin demasiado riesgo de que sean detectados.

Otras amenazas y ataques posibles

Virus ó Gusano.- (son parecidos ya que e reproducen), la diferencia es que un gusano no es un programa por sí sólo, si no que es un trozo de código que se adosa a un programa legítimo, contaminándolo.
Cuando un programa contaminado se ejecuta, ejecutará también el código del virus, lo que permitirá nuevas reproducciones, además de alguna acción (desde un simple mensaje inofensivo hasta la destrucción de todos los archivos).

Caballo de Troya. Es un programa aparentemente útil que contiene un trozo de código que hace algo no deseado.

Puerta trasera. Es un punto de entrada secreto, dejado por los implementadores del sistema para saltarse los procedimientos normales de seguridad. La puerta trasera puede haberse dejado con fines maliciosos o como parte del diseño; en cualquier caso, son un riesgo.

Caza claves. Dejar corriendo en una terminal un programa que pida "login:" y luego "password:", para engañar a los usuarios de modo que estos revelen su clave.