SEGURIDAD

Amenazas.- Para establecer una primera clasificación de tipos de amenazas en los sistemas de redes es necesario conocer los conjuntos de seguridad.

- **Confidencialidad.-** La información de un sistema deberá ser accesible solamente por grupos autorizados.
- **Integridad.**- Los elementos de un sistema de computadores solo pueden ser modificados por grupos autorizados. Ejemplo escritura, cambio de estado, borrado y creación.
- **Disponibilidad.**- Los elementos de un sistema de computadores deben estar disponibles solo para grupos autorizados.

Tipos de Amenazas

- **Interrupción.-** Es la destrucción de un elemento del sistema, esto consiste en una amenaza por ejemplo el borrado de un disco duro, o la destrucción de un archivo.
- **Intercepción.-** Sucede cuando una parte no autorizada accede a un elemento esto constituye una amenaza contra la confidencialidad por ejemplo la intercepción telefónica o la copia de un archivo.
- **Modificación.-** Es cuando una parte no autorizada accede y falsifica un elemento, es una amenaza a la integridad por ejemplo la modificación de datos de un archivo o la alteración de un programa.
- **Invención.-** Resulta de la inserción de objetos falsos al sistema, también es una amenaza a la integridad por ejemplo la inserción de mensajes falsos a la red o la inserción de archivos de registros en estado.

Tipificación.- Un tipo de amenaza son los piratas (Hacker, cracker) ellos a través de la red internet exploran las inter-redes los motivos pueden ser desde probar sus habilidades hasta hacer daños a los archivos privilegiados. Una forma de introducirse a los sistemas es mediante la obtención de contraseñas. Hay varias formas de obtener contraseñas.

- **Prueba de contraseña.-** Por omisión en las cuentas estándares que se dan junto al sistema.
- **Prueba exhaustiva.-** Se hace la prueba exhaustiva de todas las contraseñas cortas (uno a tres caracteres).
- **Pruebas de palabras.-** Probar palabras del diccionario del sistema o de una lista de contraseñas probables.

- **Reunión de información.-** Reunir información de los usuarios como por ejemplo nombres de sus esposos/as, hijos, cuadros de la oficinas libros relativos a pasatiempo, aficciones, etc.
- Probar números de teléfonos de los usuarios.
- Todos los números legales de las matriculas legales del estado.
- Emplear el caballo de Troya para saltar las restricciones.
- Intervenir las líneas entre usuarios remotos y el anfitrión.

Otro tipo de amenazas se refiere a programas sofisticados que atacan los puntos vulnerables de sistemas informáticos tanto en software de aplicación como en software de base, entre los más conocidos se encuentran las bacterias, es un programa que consume recursos del sistema y se reproduce a sí mismo.

- **Bomba Lógica.-** Es una rutina incrustada en un programa del computador que se activa cuando se presenta ciertos tipos de conjunto de condiciones en el sistema.
- **Caballo de Troya.**- Es una rutina secreta incrustada en un programa útil del usuario que cuando se ejecuta ese programa también se ejecuta la rutina.
- **Virus.**- Es un código incrustado en un programa que ocasiona que se reproduzca en otros programas realizando funciones no deseadas o perjudiciales.
- **Gusano.**- Es un programa que se reproduce y envía copias mediante las conexiones a otros computadores, además pueden realizar acciones perjudiciales.

PROTECCION

Hay varias estrategias para contrarrestar las amenazas a los sistemas de un computador.

- **Sistemas de confianza.-** Es una manera de proteger los datos o los recursos de un sistema en base a niveles de seguridad como ser la organización de información por categorías, los usuarios reciben autorización para acceder a ciertas categorías de datos. Este requisito se reconoce como seguridad multinivel y debe cumplir los siguientes requisitos.
    - No leer arriba.
    - No escribir abajo.
- **Cifrado.-** Es un método común de proteger la información que se transmiten por enlaces no confiables.

- La información se cifra en forma comprensible a una forma interna que es incompresible.
- Texto cifrado se puede almacenar en un archivo legible o transmitirse por canales desprotegidos.
- Para leer el texto cifrado el receptor debe descífralo para poder leerlo. Lo principal en este sistema o método es crear esquema de cifrado que sean imposible o al menos muy difíciles de romper. Hay diferentes métodos de cifrados los cuales consiste en:
  - Algoritmo de cifrado **E.** k
  - Algoritmo de descifrado general **D.**
  - **D(Ek(m)) = m.**
  - **Ek y Dk** calculan en forma eficiente
  - **Seguridad.-** Clave.
  - **DES.**- Data Encryption Estándar.
  - **Firewall.**

PROTECCION

Objetivo de la protección.- El papel de protección de un sistema operativo es establecer un mecanismo para hacer cumplir las políticas que gobiernan el uso de los recursos, algunas políticas están determinadas en el diseño del sistema y otras la formulan los administradores del sistema incluso hay una parte definida por los usuarios individuales, un principio importante es la separación entre política y mecanismo, los mecanismos determinan como se hacen las cosas y en contrastes las políticas definen que cosa ser harán. La separación entre política y mecanismo es importante para lograr la flexibilidad, probable que las políticas cambien de un tiempo a otro y en el peor de los casos un cambio de política requerirá un cambio en los mecanismos, son preferibles aquellos mecanismos que son generales.

DOMINIO DE PROTECCIÓN

Un sistema de comunicación es un sistema de comunicación de procesos y objetos, por ejemplo un objeto puede ser la CPU, segmento de memoria, impresoras, discos, unidad de cintas y también de software de archivos, programas y semáforos, es obvio que a un proceso solo se debe permitir el accesos a los recursos que está autorizado, ese requisito se conoce como el *principio de necesidad de conocer.* Es útil para administrar la cantidad de daños que un proceso que falla podría causar el sistema.

Un proceso opera dentro de un dominio de protección, cada dominio define un conjunto de objetos y los tipos de operaciones que se pueden realizar en el objeto, un dominio es una conexión de derechos de acceso, casa uno de los cuales es un

par ordenado <nombre de objeto, conjunto de derechos> por ejemplo si el dominio "D" tiene el derecho <archivo F {leer, escribir}>. Un proceso que se ejecute en el dominio "D" podrá leer y escribir en el archivo F y ninguna otra operación es permitida.

MATRIZ DE ACCESO

Esta matriz consiste de filas que representan dominios y las columnas objetos, cada entrada de la matriz es un conjunto de derechos de acceso, por ejemplo la entrada "acceso (i, j)" define el conjunto de operaciones que un proceso que ejecuta en el dominio Dj puede invocar con el e objeto Oj por ejemplo consideremos la matriz de acceso que tiene un dominio y 4 objetos F1, F2, F3 que son tres archivos y una impresora láser, cuando un proceso se ejecuta en el dominio D1 puede leer los archivos F1 y F3 y solo los procesos que se ejecutan con el dominio D2 tienen acceso a la impresora.

El esquema de matriz de matriz de acceso nos proporciona el mecanismo para especificar diversas políticas, el mecanismo consiste en implementar la matriz de acceso y asegurar que realmente las propiedades semánticas que acotejamos es decir asegurar un proceso que se ejecuta en el dominio Di pueda acceder solo a los objetos específicos de la fila 'i' tal cual lo definen la entrada de la matriz de acceso.

SEGURIDAD

Validación.- Generalmente la validación se basa en uno o más elementos que pueden ser:

- **Posesión del usuario.-** (Llave o tarjetas).
- **Atributo.**- (Huella dactilar, patrón de retina, firma).

- **Contraseñas.**- Es común el uso de contraseñas para proteger objetos del sistema, entonces podría asociarse una contraseña a cada recurso, podrían asociarse diferentes contraseñas a diferentes derechos de accesos.
- **Vulnerabilidad de las contraseñas.**- Los problemas de las contraseñas se asocian con la dificultad de mantener secreto la contraseña, una forma de eliminar una contraseña es el conocimiento de usuario.
- **Conocimiento.**
- **Fuerza bruta.-** Probando todas las combinaciones de letras, número, y signos de interrogación o puntuación hasta hallar la contraseña, mientras más cortas sean las contraseñas tiene menos opciones para impedir que se las adivinen mediantes intentos repetidos. Por ejemplo una contraseña de 4 dígitos solo tiene 10000 variaciones y en promedio bastarán 5000 pruebas para lograr un acierto, con un programa que prueba una contraseña cada milisegundo solo se necesitan 5 segundos para adivinar una contraseña. Las contraseñas son menos susceptibles a ser adivinadas tanto por enumeración con la distinción de mayúsculas y minúsculas, incluso todos los signos de puntuación e interrogación lo que haces mucho más difícil adivinar la contraseña.

CONTRASEÑAS CIFRADAS

Cada usuario tiene una contraseña y el sistema contiene una función extremadamente difícil de invertir pero fácil de calcular, es decir dad un valor ‘x’ es fácil calcular la función f(x) pero dado un valor f(x) es imposible calcular ‘x’ esta función se utiliza para calcular todas las contraseñas codificadas así. Cuando un usuario presenta una contraseña se codifica y es comparada con la que esta codificada y almacenada, aun si se logra descubrir esta última no podrá decodificarse y no determinar la contraseña, este modo no es necesario mantener en secreto el archivo de contraseñas. La función f(x) siempre es un algoritmo de cifrado que se ha diseñado y se ha probado rigurosamente, este método es detecto y que el sistema ya no tiene el control sobre las contraseñas. Cualquiera que tenga el archivo de cifrado podrá ejecutar rutinas de cifrado rápido y verificar los resultados con este archivo una buena técnica es generar contraseñas usando la primera letra de cada palabra de una palabra fácil de recordar, usando mayúsculas y minúsculas usando números, signos de puntuación o interrogación por ejemplo ‘EndmpeB’.

CONTRASEÑA DE UN SOLO USO

Cuando un SO inicia una sesión selecciona la azar y presenta una parte de un par de contraseñas, el usuario deberá presentar la otra parte, se podría usar un algoritmo como contraseña por ejemplo el sistema selecciona un entero y le presenta al usuario, el usuario aplica la función y responde con el resultado correcto, entonces el sistema aplica la función y si los dos resultado coinciden se permite el acceso. En este sistema de contraseña de un solo uso la contraseña es diferente para cada sesión, entonces cualquiera que pueda capturar la contraseña de una sesión y trate de usar en otra sesión fallará.

AMENAZA POR PROGRAMA

Se refiere al caso en que un programa escrito por un usuario sea utilizado por otro usuario y a raíz de esto surja un comportamiento inesperado y dañino, dos métodos comunes para causar este comportamiento se llama caballo de Troya y puerta secreta.

AMENAZA AL SISTEMA

La mayoría de los sistemas de cómputo tienen un mecanismo para que un proceso enfrente a otros procesos ejemplo los gusanos y los virus usan este mecanismo para crear una situación en la que se abuse de los recursos del sistema y de los archivos del usuario.

VIGILANCIADE AMENAZA

Un ejemplo de este método es que un sistema de tiempo compartido se cuenta las veces que se proporciona contraseñas incorrectas, las computadoras conectadas en red son muchas más susceptibles a ataques contra la seguridad en comparación con sistemas autónomos, pues los sistemas son tan seguros como la conexión más lejana del sistema. Una solución es emplear una pared cortafuegos (firewall) y así separar los sistemas de los que se confía y en los sistemas en que no se confía, una pared cortafuegos es un conmutador o un en caminador que se coloca entre los confiables y los no confiables.

CIFRADO

Es un método común de proteger información que se transmiten por los enlaces no confiables, hay varios métodos para lograr estos objetivos, los más comunes consisten en la aplicación de algoritmo de cifrado general (E),(D) y una o más claves secretas proporcionada

1. Por ejemplo sean Ex y Dk los algoritmos de cifrado y descifrado el algoritmo de cifrado debe satisfacer para un cifrado m' 1 = Dk(Ex(m)) = m.
2. Tanto en Ex como en Dk se puede calcular de forma eficiente.
3. La seguridad del sistema depende únicamente de mantener en secreta la clave y no depende de mantener en secreto lo algoritmos E y D, un algoritmo que es casi imposible de romper donde la clave de cifrado publica es un par (e, m) la clave de cifrado privado es un par (d,n) donde d y n son enteros positivos, cada mensaje se representa como entero entre (0 y (n - 1)) un mensaje largo puede dividirse en una serie de mensaje mas pequeños, las funciones E y D se definen como: E(m) = m^e mod n = c, D(c) = c^d mod n = m. el problema principal es solucionar el cifrado y descifrado, el entero n se calcula con el productos de dos números primos **p** y **q** grandes escogidos al azar y debe ser un entero grande primo que satisfaga máximo común divisor (d,(p-q)*(q -1)) = 1 y por último el entero que se calcula a partir de p y q y d como el inverso multiplicativo d modulo (p-1)*(q -1) o sea que e satisfaga e*d mod (p -1)*(q -1) = 1 a pesar que n se conoce públicamente pero p y q no se conoce públicamente.

CLASIFICACIÓN DE SEGURIDAD DE COMPUTADORAS

Los criterios de evaluación de la confiabilidad de sistema de computación de acuerdo al departamento de defensa de los EEUU específica y emisiones de seguridad en los sistemas (A, B, C, D) donde la clasificación más baja es D o sea de protección mínima, esta división comprende solo una clase y se aplica a sistemas que se evaluaron pero que no se lograran satisfacer los requisitos de cualquiera de las otras frases A, B, C tienen mayor seguridad.

TEMA # 3

RENDIMIENTO

EVALUACION DEL RENDIMIENTO

Para los diseñadores de sistemas operativos es mayor importante determinar la efectividad con la que se administran los recursos de un sistema computacional, los primeros años el mayor costo invadió en el hardware por lo que procuraba obtener un rendimiento máximo, luego se fue decrementando el costo del hardware y a su vez se fue incrementando el costo relativo del software (sistemas operativos de multiprogramación, multiprocesos y sistemas distribuidos, comunicación de datos, base de datos) que representa un porcentaje cada vez mayor en el presupuesto de un sistema de computación.

CONSIDERACION DE ASPECTOS QUE AFECTAN EN EL RENDIMIENTO.

- **Abaratamiento del hardware.-** Con el avance de la tecnología han tenido como efecto un incremento en los costos de trabajo por lo que el rendimiento de hardware base debe considerarse bajo con perspectiva de productividad humana.
- **La aparición del microprocesador.-** Esto ha ocasionado que los costos de CPU pueda establecerse nominalmente, mientras otros costos relativos a los dispositivos de entrada y salida se mantienen altos.
- **Los microprocesadores.-** Tienen una gran importancia en cuanto a su disponibilidad respecto a otros factores (CPU, E/S, Etc.).
- **Las Redes y el procesamiento distribuidos.-** Estos influyen sobre la evaluación del rendimiento, pues una red permite la optimización de una gran variedad de sistemas computacionales y recursos.

NECESIDAD PARA EL CONTROL Y EVALUACIÓN DEL RENDIMIENTO.

La evaluación puede considerarse bajo tres objetivos.

1. **Selección.-** El evaluador debe decidir sobre la conveniencia para la adquisición de un sistema de computación en particular.
2. **Proyección del rendimiento.**- Se deberá estimar el rendimiento de un sistema inexistente ya sea componentes del software o hardware.
3. **Control.**- El control de rendimiento se hace en base a datos estadísticas del sistema o de componentes para verificar las metas del rendimiento y estimar el impacto de los cambios planteados.

MEDICION DE HERD

Se refiere al modo o eficiencia con lo que un sistema de computación cumple sus metas en general, se usan cantidades relativas dependiendo además del punto de vista de espectador, la medidas más comunes del rendimiento son:

I. **Tiempo de retorno.-** Se refiere al tiempo que transcurre desde el momento en que se emite un trabajo hasta obtener todos los resultados.
II. **Tiempo de Respuesta.**- Es el tiempo que transcurre desde que el usuario aprieta la tecla ENTER hasta que empieza a imprimir una respuesta.
III. **Tiempo de reacción del sistema.**- Es el tiempo transcurrido desde que el usuario aprieta la tecla ENTER hasta la primera sesión de tiempo de servicio a la petición del usuario.
IV. **Varianza de los tiempos de respuesta.**- Se define como una media de dispersión, se aplica a cualquier variable aleatoria.
V. **Capacidad de ejecución.**- Es la cantidad de trabajo que se ejecutan en una unidad de tiempo.
VI. **Carga de Trabajo.**- Es la cantidad actual de trabajo en el sistema.
VII. **Capacidad.**- Es el máximo rendimiento que un sistema puede tener.
VIII. **Utilización.**- Es la fracción de tiempo que un recurso se utiliza.

TECNICAS DE EVALUACION DEL RENDIMIENTO

I. **Tiempos.-** Permiten comparaciones rápidas del HW (Mbps) en general se utilizan unas cuantas operaciones básicas del HW por ejemplo la suma y la negación conjunto de operaciones con cientos de operaciones diferentes, por lo tanto la información que proporciona esta técnica puede ser insuficiente.
II. **Mesclas de Instrucciones.-** Es una técnica que unas un promedio ponderado de varios tiempos de instrucciones que sean las más apropiadas para una aplicación determinada, podría ser altamente subjetiva, no proporciona información para evaluar el software puede haber también influencia de la memoria cache y canalización.
III. **Programas de Núcleo.-** Las anteriores técnicas destacan solo algunos aspectos del conjunto de instrucciones, un programa núcleo se refiere a un programa típico que puede ser ejecutado en una instalación, se cronometra la ejecución del programa núcleo en la máquina que requiere probarse y se compara con los tiempos dados por el fabricante, los programas núcleos son programas completos utilizados para evaluar componentes del software pero requiere un esfuerzo considerable y tiempo de preparación.
IV. **Métodos analíticos.-** Son representaciones matemáticas de sistemas de computación o de componentes (teoría de colas, procesos markaw) son

para evaluadores orientados a los matemáticos. Resultan fácil de crear u modificar solo hay soluciones claras para los modelos más simples.

V. **Puntos de referencia.-** Es un programa real de comparación de rendimiento que es ejecutado en la máquina que se está evaluando. En general se trata de un programa de producción, sirve para evaluar tanto el HW como el SW probablemente es la técnica más utilizada para la adquisición de equipos computacionales de varios proveedores diferentes.

VI. **Programas Sintéticos.-** Combinan técnicas de los núcleos y los puntos de referencia, son diseñados para probar características específicas de una nueva máquina, requiere de mucho tiempo de codificación y depuración.

VII. **Simulación.-** Para la utilización de esta técnica hay que desarrollar un módulo computarizado del sistema que se quiere evaluar, se aplica mucho en la industria espacial y de transporte, se ejecutan ya sea por eventos o por vibretos, requiere mucha experiencia del evaluador, una vez desarrollado el simulador del módulo su uso respectivo es fácil y económico.

VIII. **Control del rendimiento.-** Consiste en la recolección y análisis de información en sistemas ya existentes con el fin de evaluar la capacidad de ejecución tiempo de respuesta, etc. Puede localizar embotellamientos y mostrar una forma de mejorar el rendimiento. El control de rendimiento se lo puede hacer mediante técnicas del hardware o software, se pueden utilizar monitores de software, son más económicos pero podrían distorsionar los resultados, los monitores de hardware son más costosos pero dan resultados exactos.

EMBOTELLAMIENTO Y SATURACIÓN

Un sistema computacional es una colección de recursos que es administrada por el sistema operativo, cuando algún recurso llega al límite de su capacidad significa que se encuentra saturado, en este punto dicho recurso produce un embotellamiento puesto que lo usa de peticiones a ese recurso, es mayor su uso de servicio y los procesos que compiten por la obtención de ese recursos se interfieren unos con otros, estos tiene un efecto en los demás recursos del sistema porque interactúan en forma compleja dando como resultado una disminución en la capacidad de rendimiento, una forma de eliminar los embotellamientos es aumentando los recursos o aumentando su capacidad.

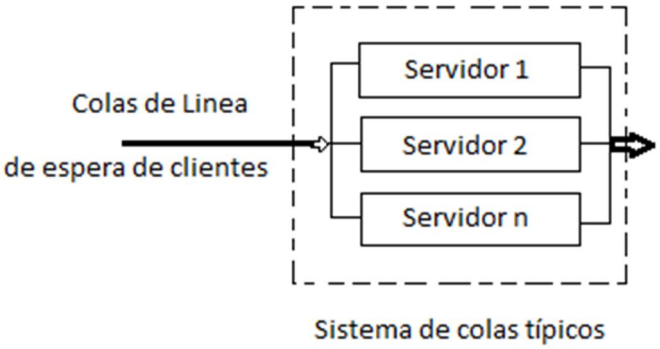
CICLO DE REALIMENTACIÓN

Consiste en la reutilización de la información del estado actual del sistema como contribución como contribución a las entradas posteriores, la retro-alimentación es negativa cuando da como resultado el decremento de las tasas de entrada y es positivo cuando tiene como efecto el incremento de las tasas de entrada por ejemplo una retro-alimentación negativa son las salidas del spool en los sistemas operativos estas salidas pueden ser impresas en cualquiera de las diferentes impresoras que sea equivalente, cuando la cola de una impresora es demasiado largo este puede ser llevado a otra cola. La retro-alimentación negativa contribuye a la estabilidad del sistema de colas, con ejemplo de retro-alimentación positiva es la que se produce en los sistemas de programación de memoria virtual (primera versión) en este caso que el sistema operativo detectaba que la CPU no era usada de acuerdo a su capacidad entonces el planificador incrementaba el nivel de multiprogramación, este incremento de trabajos ocasionaba una disminución en la memoria asignada a cada trabajo y por lo tanto un aumento y fallo de página dando como resultado una disminución en la utilización de la CPU. La retroalimentación positiva provoca el incremento de algún parámetro y puede causar inestabilidad en los sistemas de cola.

MODELOS ANALÍTICOS

Algunas de las técnicas más populares de modelo analítico son las teorías de colas y los procesos de Markov. Los modelos analíticos son de representación matemática de los sistemas y permiten que el evaluador saque conclusiones rápidas y exactas sobre el comportamiento de un sistema.

> **>Teoría de colas.-** Matemáticamente cola significa una línea de espera. Lo ideal sería obtener de inmediato el servicio que se requiere sin que tener que formar en una línea de espera o cola; pero eso supondría un costo muy elevado de la capacidad de servicio necesario. Las colas significan el cambio de tiempo por dinero, porque el consumo de tiempo en una línea de espera significa la disminución del costo de servicio porque se hace una mejor utilización de las instalaciones del servicio. Ej. En el campo de la computación el procesamiento de una solicitud de E/S, la atención del procesador, etc.

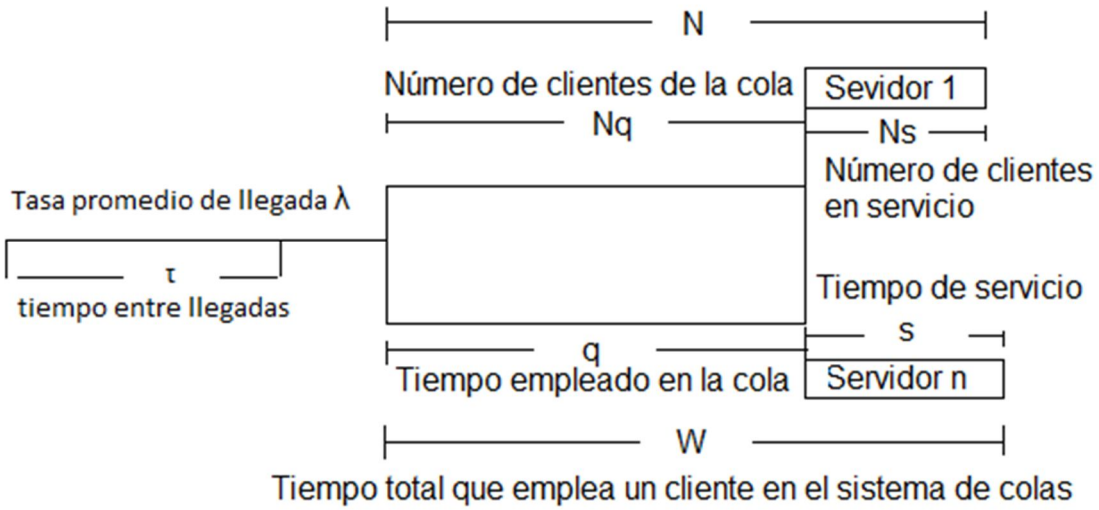


Sistema de colas típicos

En una instalación de servicio que contiene una cierta cantidad de servidores idénticos, cada uno de ellos puede proporcionar el servicio requerido al cliente. Cuando todos los servidores se encuentran ocupados y entra un nuevo cliente a la red de colas, entonces tiene que esperar hasta que se desocupe uno de los servidores.

Las colas son ilimitadas cuando pueden crecer tanto como sea necesario para contener (sujetar) a los clientes que esperan. Las colas son limitadas cuando tienen una capacidad establecida de número de clientes, quizá cero.

Para los problemas de las colas se debe tener en cuenta un número de variables aleatorias las cuales pueden ser descritas mediante distribuciones probabilísticas.



Algunos de los elementos de interés de los sistemas de colas típicos son:

a) **Fuente.-** El caudal de clientes se realiza desde una fuente la cual puede ser finita o de tamaño limitado, infinita o arbitrariamente grande.

b) **Llegadas.-** Se supone que los elementos llegan a un sistema de colas con los tiempos $t_0 < t_1 < t_2 < \ldots < t_n$. Llegan de uno en uno y no hay colisión porque los clientes intenten entrar al sistema al mismo tiempo. Las variables aleatorias $T_k = t_k - t_{k-1}$, (k>= 1). Miden los tiempos entre llegadas sucesivas y se denominan tiempos entre llegadas. Se asume que estas variables son independientes y están idénticamente distribuidas.

c) **Llegadas de Poisson.-** Las llegadas pueden ser de acuerdo a cualquier patrón arbitrario pero en la teoría de colas se supone que esas llegadas forma un "proceso de llegada de Poisson". Para ello se tiene características de que los tiempos entre llegadas están distribuidos exponencialmente. La distribución de Poisson es una distribución discreta usada en situaciones probabilísticas donde el área de oportunidad para la ocurrencia de un evento es grande pero la probabilidad de una ocurrencia en un intervalo particular o en un punto particular es muy pequeña. Algunos ejemplos tradicionales de situaciones prácticas donde la distribución de Poisson se considera aplicable son: el número de defectos en una determinada longitud de un alambre aislado, los errores de impresión cometidos por una secretaria recargada de trabajo, las imperfecciones de una placa de vidrio, accidentes industriales y llegadas en modelos de cola.

   para los ejemplos en el área de oportunidad se considera grande pero la probabilidad de una ocurrencia en un punto se considera pequeña. Matemáticamente la probabilidad de exactamente n ocurrencias de un evento, usando la distribución de Poisson es:

$$P(n) = [(\lambda * t)^n * e^{-\lambda t}]/n!$$

   Si se trata de modelo de colas:

   t : longitud del intervalo

   λ: tasa promedio de llegadas por oportunidad de tiempo.

d) **Tiempos de servicio.-** Se supone que los tiempos de servicios también son tiempos aleatorios.

   S_k: Tiempo de servicio requerido por el k-iesimo cliente.

   S : Tiempo de servicio arbitrario.

   μ: Tasa promedio de servicio.

La distribución de los tiempos de servicio con una tasa promedio de servicio μ es: $w_s(t) = p(s =< t) = 1 – e^{-\mu t}$; t >= 0.

e) **Capacidad de la cola.-**
   - **Capacidad infinita.-** Cada cliente que llega es admitido en el sistema de cola independientemente de los clientes que ya espera.
   - **Capacidad cero.-** Si los clientes que llegan no son servidos inmediatamente no podrán ser admitidos en el sistema (sistema de perdidas).
   - **Capacidad positiva.-** Los cliente que llegan solo esperan si hay lugar en la cola.

f) **Número de servidores en el sistema.-**
   - **Sistema de un solo servidor.-** Dan servicio a un solo cliente a la vez.
   - **Sistema de servidores múltiples.-** Tienen n servidores múltiples con la misma capacidad y dan servicios a n clientes a la vez.

g) **Disciplinas de colas.-** Se refiere al método utilizado para elegir al siguiente cliente de la cola que va ser servido. La más utilizada es FCFS.

h) **Intensidad de tráfico.**- Es una medida de capacidad del sistema para dar servicio ($E(s)= 1/\mu$) y la media de tiempo entre llegadas ($E(\tau)= 1/\lambda$) y la intensidad de tráfico es $U= E(s)/ E(\tau) = \lambda / \mu$. Esta medida es útil para determinar el número mínimo de servidores que necesitará un sistema para dar servicios a sus clientes sin que las colas hayan indefinidamente largas o simplemente rechazar clientes.

i) **Utilización del servidor.-** Se refiere a la probabilidad de que un servidor determinado se encuentre ocupado (p). la ley de los grandes números establece que esta es aproximadamente la fracción de tiempo que cada servidor esta en uso. Para un sistema de un solo servidor la utilización del servidor es igual a la intensidad de tráfico. $P = U/c = \lambda / \mu c$. donde c es número de servidores, U es intensidad de tráfico, λ tasa promedio de llegada de clientes.

j) **Estado estable en función de soluciones transitorias.**- Cuando un sistema se inicia por primera vez transcurre un periodo inicial que por lo general no es indicativo de su comportamiento periódico (Ej. Vuelo de avión entre dos aeropuertos). Los sistemas de cola deben pasar por un periodo inicial de operación antes de tener un funcionamiento uniforme y predecible. Para hacer un estudio de un sistema es necesario que este se encuentre en estado estable, porque allí es donde sus parámetros importantes permanecen fijos y resulta sencillo categorizar la operación del sistema. Las soluciones transitorias o dependientes del tiempo son muchos mas complejas.

k) **Resultados de Little.**- Se usa para medir el rendimiento de un sistema de cola y se destaca por su sencillez y utilidad.
   - Wq = Tiempo promedio que emplea un cliente en la cola.
   - W = Tiempo medio que emplea un cliente en el sistema.
   - Lq = Número de clientes en la cola.

- L = Número de clientes en el sistema.
- Λ = Tasa de llegadas.

> Procesos de Markov.- Los procesos de Markov de primer orden, pueden usarse como modelos de un proceso físico o económico con las siguientes propiedades.

a) El conjunto de sucesos es finito.
b) La probabilidad del siguiente suceso depende solamente del suceso inmediatamente anterior.
c) Estas probabilidades permanecen constante en el tiempo.

Cada suceso individual se denomina un estado. Esto significa que habrá tantos estados como sucesos posibles. Si: i-esimo estado de m posibles; $2 <= m < \infty$.

>> Definiciones.-

a) Un estado Sj es transitorio, si desde un estado Sk alcanzado des Sj, el sistema no puede regresar a Sj
b) Un estado Sj es recurrente, si desde cada estado Sk alcanzable desde Sj, el sistema puede regresar a Sj.
c) Una cadena sencilla es un serie de estados recurrentes tal, que el sistema pueda llegar a cualquier estado de la cadena desde cualquier otro estado de esta.
d) Un cambio de estado en un proceso de Markov de transición continua, puede producirse en cualquier instante de una escala de tiempo continua.

>> Procesos de nacimiento y muerte.-Es un caso importante de los procesos de Markov y es especialmente aplicable al modelado de sistemas de computación y son más fáciles de resolver. Este tipo de proceso tiene la propiedad. Que:

$$\Lambda_{ij} = 0 \text{ si } j \neq i+1 \text{ y } j \neq i-1$$

TEMA NRO 3

SISTEMA OPERATIVO UNIX