

U.A.N.L.

Facultad de ciencias Físico-Matemático

Nombre del alumno: Jorge Mario Quintanilla Rios

Nombre del maestro: Ing. Miguel Salazar

Nombre de la asignatura: DOO (Diseño Orientado a Objetos)

Grupo:

Salón:

Numero de tarea: #3

|  |  |  |
| --- | --- | --- |
| Nombre | ¿Que es? | ¿Cómo funciona? |
| Aplicaciones Moviles | Una app es una aplicación de software que se instala en dispositivos moviles o tablets para ayudar al usuario en una labor concreta | Necesitas un smartphone, una tablet o algún otro dispositivo móvil con acceso a internet. Para los sistemas operativos móviles Android, Apple, Microsoft y BlackBerry hay tiendas de aplicaciones (app stores en inglés) que operan en línea en las cuales puedes buscar – y también descargar e instalar – las aplicaciones. Debes de usar una tienda que te ofrezca las aplicaciones que funcionan con el sistema operativo de tu dispositivo. |
| Aplicaciones web | Se llaman asi porque trabajan sobre internet y los datos y los archivos en los que trabajas son procesados y almacenados dentro de la web. El concepto de aplicaciones web esta relacionado con el almacenamiento en la nube. Toda la información se gurda de manera permanente en grandes servidores de internet y los datos requeridos en ese momento quedando una copia temporal dentro del equipo | El usuario interacciona con las aplicaciones Web a través del navegador. Como consecuencia de la actividad del usuario, se envían peticiones al servidor, donde se aloja la aplicación y que normalmente hace uso de una base de datos que almacena toda la información relacionada con la misma. El servidor procesa la petición y devuelve la respuesta al navegador que la presenta al usuario. Por tanto, el sistema se distribuye en tres componentes: el navegador, que presenta la interfaz al usuario; la aplicación, que se encarga de realizar las operaciones necesarias según las acciones llevadas a cabo por éste y la base de datos, donde la información relacionada con la aplicación se hace persistente. Esta distribución se conoce como el modelo o arquitectura de tres capas. |
| Aplicaciones de escritorio | Son las que se encuentran instaladas en el ordenador o sistemas de almacenamiento (USB) y esposible ejecutarlo sin internet en nuestro sistema operativo. | Es un tipo de software que funciona como un conjunto de herramientas diseñado para realizar tareas y trabajos específicos en tu computador. |
| Aplicaciones de consola | Se le define aplicación de consola como aquella que se ejecuta en una ventana de MS-DOS o línea de comandos. | Se utiliza un IDE llamado Visual basic.  Y se le considera un lenguaje backend |
| Daemons(procesos en background) | se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de programas continua en el sistema, es decir, que puede ser ejecutado en forma persistente o reiniciado si se intenta matar el proceso dependiendo de la configuración del demonio y de las políticas del sistema. | Funciona de manera automática para que se ejecute de manera correcta algún proceso. |
| Tipos de malware | Virus clásicos. Programas que infectan a otros programas por añadir su código para tomar el control después de ejecución de los archivos infectados. El objetivo principal de un virus es infectar. La velocidad de propagación de los virus es algo menor que la de los gusanos.  Gusanos de red. Este tipo de malware usa los recursos de red para distribuirse. Su nombre implica que pueden penetrar de un equipo a otro como un gusano. Lo hacen por medio de correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos (P2P), canales IRC, redes locales, redes globales, etc. Su velocidad de propagación es muy alta.  Al penetrar un equipo, el gusano intenta obtener las direcciones de otros equipos en la red para empezar enviarles sus copias. También suelen usar los datos del libro de contactos del cliente de correo electrónico. La mayoría de los gusanos se propagan en forma de archivos pero existe una pequeña cantidad de gusanos que se propagan en forma de paquetes de red y penetran directamente la memoria RAM del equipo víctima, donde a continuación ejecutan su código.  Caballos de Troya, troyanos. Esta clase de programas maliciosos incluye una gran variedad de programas que efectúan acciones sin que el usuario se dé cuenta y sin su consentimiento: recolectan datos y los envían a los criminales; destruyen o alteran datos con intenciones delictivas, causando desperfectos en el funcionamiento del ordenador o usan los recursos del ordenador para fines criminales, como hacer envíos masivos de correo no solicitado.  No son virus clásicos porque no infecta otros programas o datos. Los troyanos no pueden penetrar a los equipos por si mismo, sino se propagan por los criminales bajo la vela de algún software “deseable”. Son capaz de causar mucho más daño que los virus clásicos.  Spyware. Software que permite colectar la información sobre un usuario/organización de forma no autorizada. Su presencia puede ser completamente invisible para el usuario.  Pueden colectar los datos sobre las acciones del usuario, el contenido del disco duro, software instalado, calidad y velocidad de la conexión, etc.  Pero no es su única función. Son conocidos por lo menos dos programas (Gator y eZula) que permiten también controlar el equipo. El otro ejemplo de programas espías son los programas que instalan su código el navegador de Internet para redireccionar el tráfico. Posiblemente haya visto cómo funcionan, cuando en cambio de la página web solicitada se abre una otra.  Phishing. Es una variedad de programas espías que se propaga a través de correo. Metan recibir los datos confidenciales del usuario, de carácter bancario preferente. Los emails phishing están diseñadas para parecer igual a la correspondencia legal enviada por organizaciones bancarias, o algunos brands conocidos. Tales emails contienen un enlace que redirecciona al usuario a una página falsa que va a solicitar entrar algunos datos confidenciales, como el numero de la tarjeta de crédito.  Adware. Muestran publicidad al usuario. La mayoría de programas adware son instalados a software distribuido gratis. La publicidad aparece en la interfaz. A veces pueden colectar y enviar los datos personales del usuario.  Riskware. No son programas maliciosos pero contienen una amenaza potencial. En ciertas situaciones ponen sus datos a peligro. Incluyen programas de administración remota, marcadores, etc.  Bromas. Este grupo incluye programas que no causan ningún daño directo a los equipos que infectan. No obstante, muestran advertencias falsas sobre supuestos daños ocurridos o por ocurrir. Pueden ser mensajes advirtiendo a los usuarios de que los discos se han formateado, que se ha encontrado un virus o se han detectado síntomas de infección. Las posibilidades son limitadas sólo por el sentido del humor del autor del virus.  Rootkits. Un rootkit es una colección de programas usados por un hacker para evitar ser detectado mientras busca obtener acceso no autorizado a un ordenador. Esto se logra de dos formas: reemplazando archivos o bibliotecas del sistema; o instalando un módulo de kernel. El hacker instala el rootkit después, obteniendo un acceso similar al del usuario: por lo general, craqueando una contraseña o explotando una vulnerabilidad, lo que permite usar otras credenciales hasta conseguir el acceso de raiz o administrador.  Otros programas maliciosos. Son una serie de programas que no afectan directamente a los ordenadores, pero que se usan para crear virus, troyanos o para realizar actividades ilegales como ataques DoS y penetrar en otros ordenadores, etc.  Spam. Los mensajes no solicitados de remitente desconocido enviados en cantidades masivas de carácter publicitario, político, de propaganda, solicitando ayuda, etc. Un otro clase de spam hacen las propuestas relacionadas con varias operaciones ilegales con dinero o participación en algún supernegocio. También hay emails dedicados a robo de contraseñas o números de tarjetas de crédito, cartas de cadena, etc. Spam genera una carga adicional a los servidores de correo y puede causar pérdidas de la información deseada. |  |