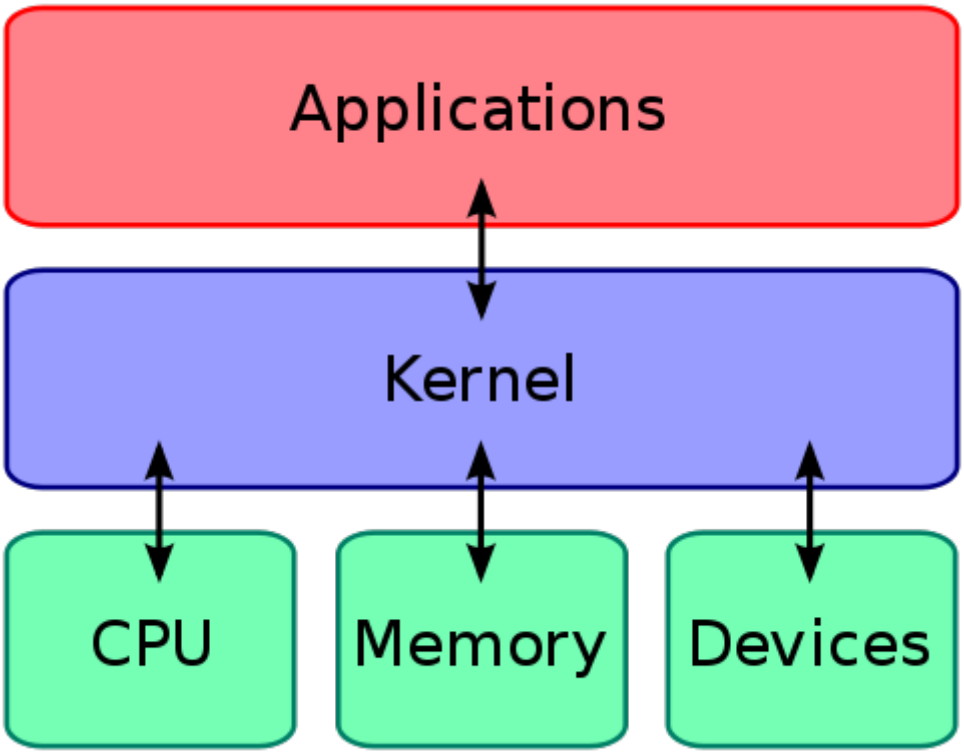
Gracias a todos los que participan en el curso. Quiero comentar que hay un grupo en Skype, para el que quiera. Pueden mandarme un mail para que los agregue en caso de que quieran:).

Ya estuvimos viendo la historia del famosísimo sistema operativo. Claro que fue resumida y todo, pero no nos dejamos de lado nada importante.

Bueno, vamos a introducirnos un poco más a fondo.:)

"Roadd, siempre me hablan y me cuentan de un tal kemel o no se qué. ¿De qué están hablando?"

¡Manolo! Mira si no te íbamos a extrañar. Te cuento que de lo que hablan se llama **kernel**. El kernel -también llamado **núcleo**-, es un **software** indispensable para el sistema operativo. Éste corre con **privilegios** elevados y es el encargado de **administrar** los **recursos** de hardware a los software que corren en el sistema. Como si éste dijese: "Paint, te doy 2 mb de RAM durante 2 horas. Word, a vos te doy 10 mb de Ram y 50 mb de espacio en disco." Y así, sucesivamente con cada programa que corre para hacer un uso correcto de los recursos, que sino se gastarían rápidamente.
A parte, para los **programadores**, les deja formas fáciles para que puedan dar comandos de bajo nivel al hardware presente y no se les haga **compleja** la tarea. No olvides, que de igual manera, ésto tiene que pasar a través del kernel.

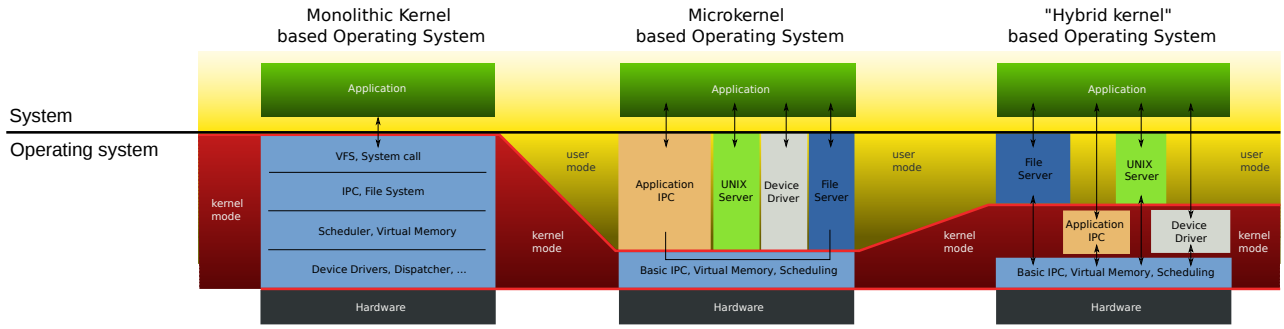


"¿Y hay distintos tipos de kernel, o es un estándar para todos?"

Excelente pregunta. Hay distintos tipos. En total, 4.
Windows, usa el **núcleo monolítico** en las versiones que estaban basadas en **MS-DOS**. Es decir que hasta el Windows Me, lo seguían usando. Un núcleo monolítico quiere decir que todas las funcionalidades que tiene se concentran sobre **un** solo gran **kernel**, con un solo **módulo**. La situación es que conlleva una gran complejidad y que esto apunta a que cada vez que hay un cambio en alguna parte del kernel, hay que **volver a compilar** todo, por lo que imagínense que habría que volver a instalar los programas y etcétera. Por ésto, los monolíticos son de un tamaño bastante **grande** con funcionalidades extra para cada hardware que exista y así no tener problemas. Con respecto a la **seguridad** también hay un **problema**. En el caso que uno de los servicios pueda llegar a tener una vulnerabilidad, se compromete todo lo demás porque comparte el módulo. Eso sí, como ventaja tenemos el rendimiento que es excelente.

Por otro lado tenemos los **microkernel**, que aunque no es usado por Windows, nos puede ayudar a entender el próximo concepto. El microkernel es de sistema **modular**, y tiene la **flexibilidad** de que muchas de las cosas que tiene conectadas las deja en modo usuario (es decir que va a ser portable mientras no cambiemos lo esencial). Éstos kernel son **livianos** y **seguros**, ya que si llegan a comprometer algo del sistema, es un simple módulo y no va más allá de eso.

Pero las nuevas versiones de Windows, que estan basadas en **NT** tienen **núcleo híbrido**, una mezcla entre las 2 que nombré anteriormente. Éste hace que la mayor cantidad de cosas de Entrada/Salida (los periféricos) y los drivers, se ejecuten en **modo usuario**, pero las cosas **importantes** ya van a nivel **elevado y corresponden a un solo módulo.**



"Ya soy todo un campeón y un experto de Windows:)"

Ay, Manolo. Te falta mucho, y más vale que lo sepas. Por ejemplo, veamos de qué se trata el **Windows Update**. Lo único que conocemos de él es que sirve para actualizar nuestro sistema operativo, ya sea para darle más y mejores **funcionalidades** o para **parchear** vulnerabilidades de seguridad.
Quizás en parámetros de funcionamiento no sea tan interesante, es un simple gestor de descargas que verifica el hardware que hay conectado, y comprueba con lo que tenemos que actualizar y lo hace. Pero hay cosas que debemos tener en cuenta. Veamos:

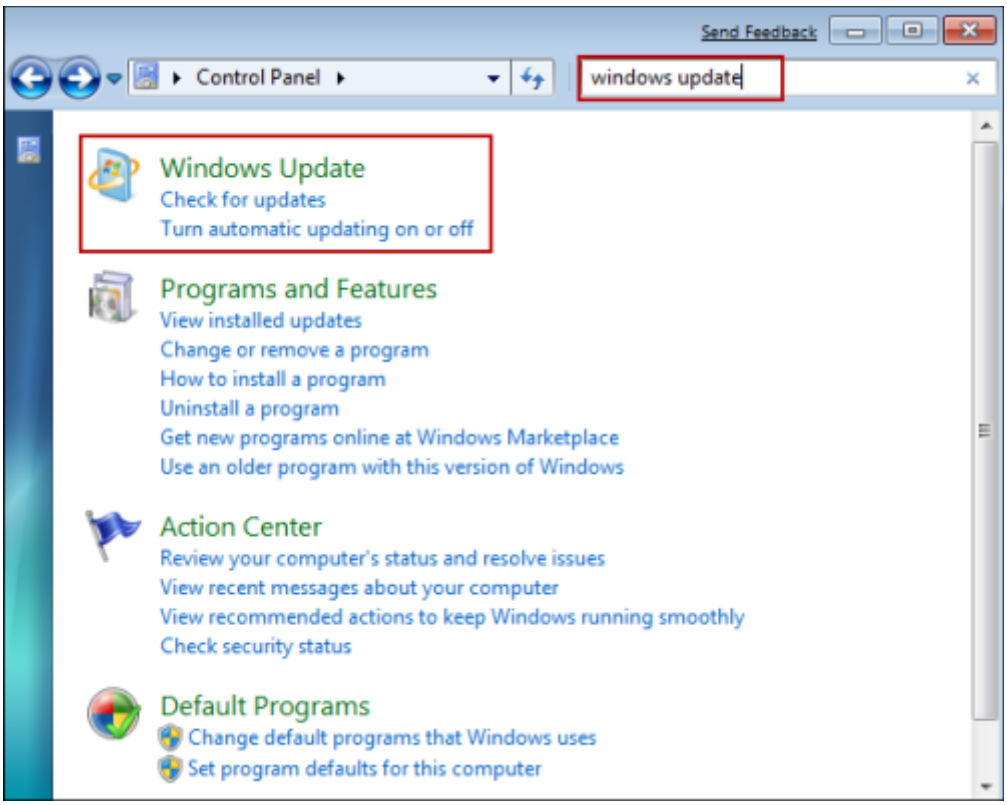
-**A menos que sea una vulnerabilidad crítica, las actualizaciones se realizan los Martes**. Claro que igualmente se pueden bajar de manera manual, entrando desde la página de MicroSoft. Así que si encontramos que una vulnerabilidad fue descubierta y MS no la toma como crítica, tenemos varios días para explotarla.

-Sacar nuevos parches o funcionalidades es **instalar nuevo código**, lo que puede indicar nuevas vulnerabilidades.

-Un gran porcentaje de personas (creo que el último censo, hace unos años, dio algo así como el 90%), usan las **actualizaciones automáticas** sin siquiera ver qué es lo que estamos instalando. Si descubriésemos una vulnerabilidad en el Windows Update o hacemos algún ataque que permitiese que el usuario descargue algo que nosotros queramos, podríamos comprometer al sistema hasta el nivel de privilegios más altos.

-Algo que hay que tener muy en cuenta. En LatinoAmerica, hay mucha **piratería** que quiere decir menos actualizaciones y más sistemas comprometidos con errores viejos de seguridad.

-La gente sabe que **actualizar es bueno** -más si hablamos de las generaciones venideras- y si en internet aparece un botón con "usted tiene errores, debe actualizar" que lo lleva a la instalación de un virus, puede ser infectado fácilmente.

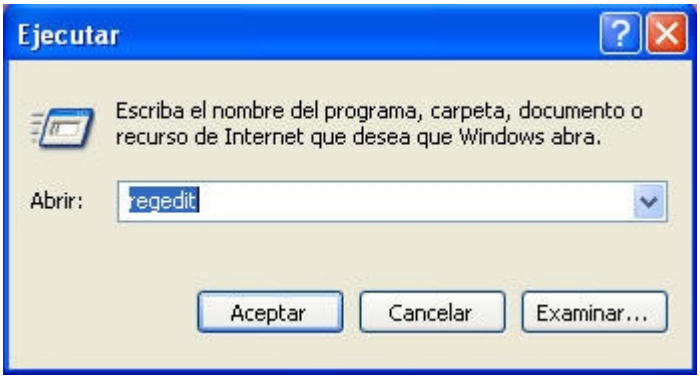


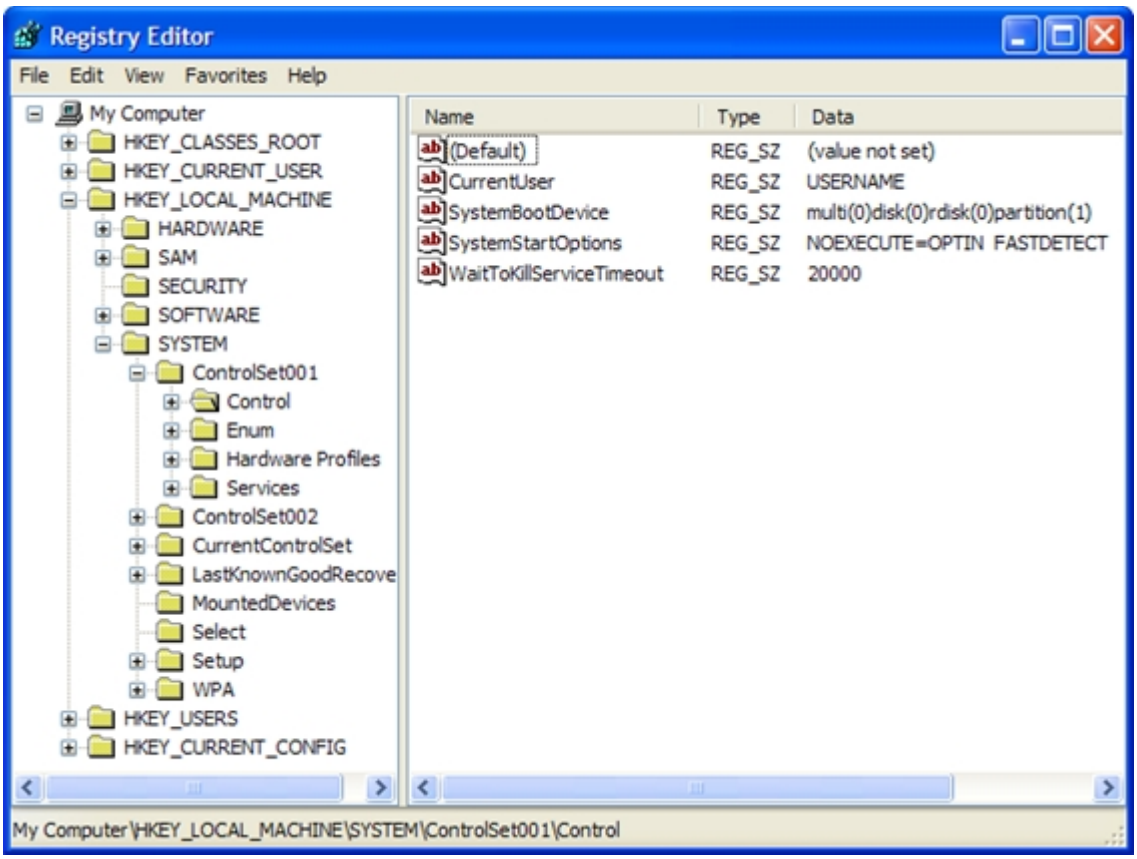
"O sea que Windows es malo."

No es que sea malo, pero cuando el humano tiene que intervenir y cuando el código está en malas manos, puede pasar cualquier cosa. Pasa en Windows y pasa en cualquier otro S.O.

Y luego, tenemos el **Registro** de **Windows**. Éste es una base de datos que contiene archivos de configuración y opciones de aplicaciones, drivers, el kernel. Para editar el registro, podemos ir a **Inicio -> Ejecutar -> regedit**.

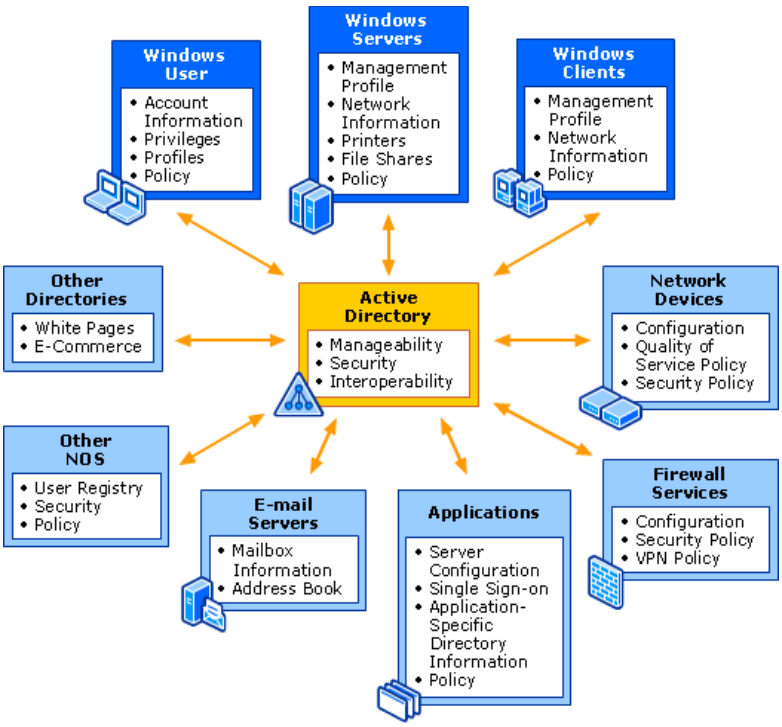
Nos abrirá una ventana como ésta, la cual aún no tocaremos porque podría generar cambios críticos al sistema y dejaría de funcionar como debe. Es sensible, así que si van a tocar, que sea con cuidado.





Un adelanto de lo que una de las cosas que nos interesa: en el Registro, tenemos los programas que **inician** con el sistema. Sería una lástima que alguien quisiera **arruinar** el inicio con un troyano ¿Verdad?

"Lo vamos a ver más adelante. Quiero que me digas algo de Active Directory. Siempre veo que piden conocimientos de ésto y no sé qué es."



Interesante. **AD**, es una **herramienta** -**software**- excelente de **Windows Server**. Se trata de una aplicación que organiza los datos de una red y puede establecer permisos de acceso a los usuarios. Algo así como una **herramienta** de **administracion** y **seguridad** de una **red**.

Ya que esto es una simple clase introductoria, dejemos la clase aquí. En las próximas clases, profundizaremos los temas. Ya casi la clase 50!:D

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:
1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
