Principios de Diseño [sistemas operativos segunda edición William stallings]

Saltzer y Shroeder identifican una serie de principios en el diseño de medidas de seguridad para las diversas amenazas a los sistemas informáticos. Estos principios fueron diseñados después de trabajar con MULTICS Entre los principios se incluyen los siguientes:

* Mínimo privilegio: Todos los programas y usuarios del sistema deben operar utilizando el menor conjunto de privilegios necesarios para complementar la labor. Los derechos de acceso deben adquirirse solo con permiso explicito; por omisión deberían ser “sin acceso”.
* Ahorro de mecanismos: Los mecanismos de seguridad deben ser tan pequeños y simples como sea posible, ayudando en su verificación. Esta exigencia suele suponer que deben ser una parte integral del diseño, más que mecanismos añadidos a diseños existentes. Dicho en otras palabras, deben de estar en los niveles más bajos del sistema. Un sistema así se podrá analizar, verificar, probar y diseñar fácilmente. Tratar de añadir seguridad a un sistema inseguro existente es casi imposible; la seguridad, al igual que la exactitud, no es una característica que se pueda agregar.
* Aceptación: Los mecanismos de seguridad no deben interferir excesivamente en el trabajo de los usuarios, mientras cumplen al mismo tiempo las necesidades de aquellos que autoricen el acceso. Si los mecanismos no son fáciles de usar, probablemente no van a ser usados o lo serán de forma incorrecta. Entre más fáciles de usar y aceptables menos posibilidades de que un usuario lo trate de evitar.
* Mediación total: Cada acceso debe ser cotejado con la información de control de acceso

incluyendo aquellos accesos que suceden fuera de la operación normal, como la recuperación y el mantenimiento. Es decir, comprobar cada acceso al sistema o en su defecto comprobar los permisos de los usuarios de forma periódica y no solo la primera vez. Ya que si esto ocurre implica que un usuario que abre un archivo y lo mantiene unido durante semanas seguirá teniendo acceso, incluso si el propietario ha modificado ya la protección del archivo.

* Diseño abierto: La seguridad del sistema no debe depender de guardar en secreto el diseño de sus mecanismos. De esta forma, los mecanismos podrán ser revisados por muchos expertos y los usuarios podrán, por tanto, depositar una alta confianza en ellos. La suposición de que los intrusos no conocen el funcionamiento del sistema sólo sirve para que los diseñadores se engañen a sí mismos. Tambien podría disuadir a posibles curiosos

Windows vs Linux

1. En Linux el usuario por defecto solo tiene privilegios de escritura en su carpeta de usuario en /home. En Windows desde un inicio se es parte del grupo de administradores.
2. En Linux la seguridad esta en el kernel y en el sistema de ficheros que contempla una jerarquía de privilegios para cada elemento del SO. En Windows esta en la capa de aplicación (antivirus) y respecto al sistema de ficheros FAT o FAT32 no tiene seguridad y NTFS está desactivada la seguridad por defecto.
3. En Windows es muy fácil debido a las interfaces y en Linux no por tener que acceder al modo root.
4. Al cuarto punto le vale el tercero ya que la “incomodidad” es necesaria pero no la merecemos como batman pero al revés. En Windows el usuario/troyano puede instalar cosas sin algún control. En Linux la instalación se hace por claves PGP y otras cosas.
5. Se refiere a software libre y ya sabemos que opina Windows al respecto

[SALT75] saltzer, J., y shroeder, M. “The protection of information in computer systems”. Proceedings of the IEEE, septiembre de 1975