Contraseñas

ROBERTO PLÀ
Comandante de Aviación
http://personal.redestb.es/pla/
pla@redestb.es

Con la implantación en todo el Ejército del Aire del sistema de interconexión a través de Lotus Notes y su apertura al sistema de correo electrónico de Internet así como a otros servicios de la red de redes, la necesidad de seguridad informática adquiere mayor relieve. Por ello seria interesante recordar una serie de normas elementales a la hora de establecer las contraseñas, en ocasiones único baluarte que defiende a un sistema de un uso ilegítimo y a nuestra información de su difusión pública o hacia destinos no deseados por nosotros.

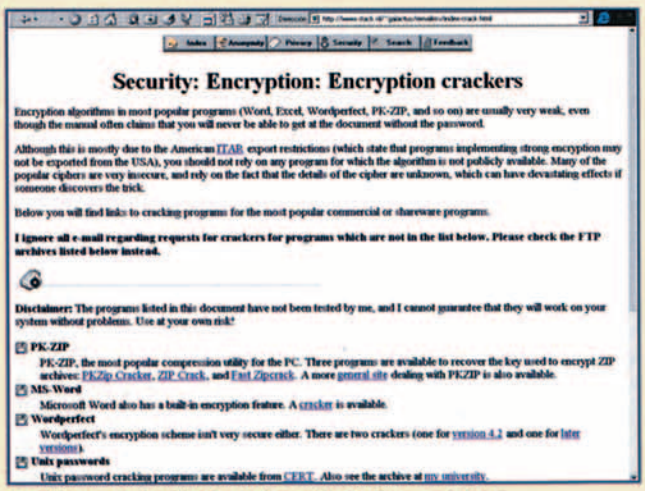
El principal y primer requisito de seguridad de una contraseña es ser establecida. Ha tenido cierta relevancia en los sectores de Internet interesados en temas de seguridad y "Hacking" los accesos no autorizados a páginas web realizadas mediante el programa de Microsoft "Front Page" debidas a la sencilla circunstancia de que sus administradores habían olvidado establecer esta barrera de seguridad. No obstante la seguridad total es opuesta a la operatividad total; Las medidas de seguridad, no deben ser tales que impidan la utilización lícita y ágil de los sistemas. En nuestro puesto de trabajo podemos establecer una clave de acceso al ordenador que debe ser conocida por el coordinador de informática o la persona responsable que este determine a fin de que la ausencia de un usuario o el olvido de la clave por parte de este no derive en daño para la información guardada en el ordenador.

Cuando tengamos que establecer una contraseña segura tendremos que tener en cuenta que esta debe ser lo mas larga que el sistema permita y seamos capaces de recordar y formada por una serie de caracteres alfanuméricos lo más aleatorios posible. En estudios realizados se ha demostrado que el número de palabras 'ingeniosas' utilizadas por los usuarios es muy corto y los fallos mas frecuentes consisten en usar como clave el propio identificativo del usuario, el apellido o el nombre de la esposa y palabras como 'secreto', 'administrador', 'dios', 'sexo'...

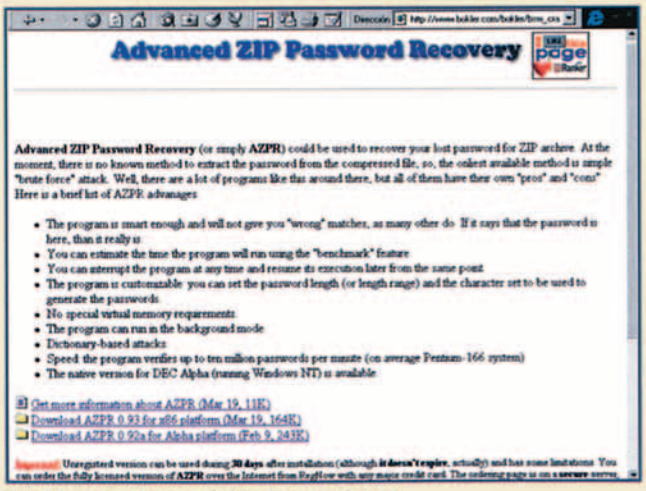
En este sentido es aconsejable no utilizar ni tan siquiera palabras que existan en el diccionario, preferentemente de ningún idioma.

Cualquier combinación, por ingeniosa que nos parezca de nuestro nombre, el de familiares las onomásticas o fechas memorables, los nombres de nuestros familiares, de la unidad, nuestro indicativo personal el número de filiación de la academia, el del ISFAS o el del DNI, la mezcla de varios de estos datos o de fragmentos de ellos debe ser desechada. Los intrusos son muy ingeniosos y cualquiera que haya mandado tropa sabe que es muy difícil ser original e inventar algo realmente nuevo.

Nos tropezamos entonces con la dificultad de recordarlas, por lo que es un truco frecuente usar palabras comunes desfigurándolas, mediante una 'falta de ortografía' o bien sustituyendo algunas de sus letras por números de grafía similar como la 'o' por el cero, la 'e' por el tres, así podemos usar "35ta1la" por 'estalla', 'dtrminad0$' por 'determinados'. Como todos aquellos que han tenido que memorizar los procedimientos de un avión saben se pueden usar iniciales de una frase para formar la palabra clave como unas siglas: 'edvenedraya' por "Estoy Deseando Ver El Nuevo Ejemplar De Revista Aeronáutica Y Astronáutica', de forma que se convierte en algo más sencillo y más fácil de memorizar que si se trata de una serie de letras y cifras sin sentido alguno.



http://www.stack.nl/~galactus/remailers/index-crack.html
Enlaces a programas para obtener el password de procesadores de texto, archivos Zip, Sistemas UNIX y otros.



http://www.bokler.com/bokler/bsw_crak.html
Software que nos permite recuperar informacion comprimida en un archivo ZIP cuando hemos olvidao el password con el que la protegimos.

http://www.crack.com/
Compañia comercial que ofrece software para romper protecciones basadas en contraseña en diversas aplicaciones

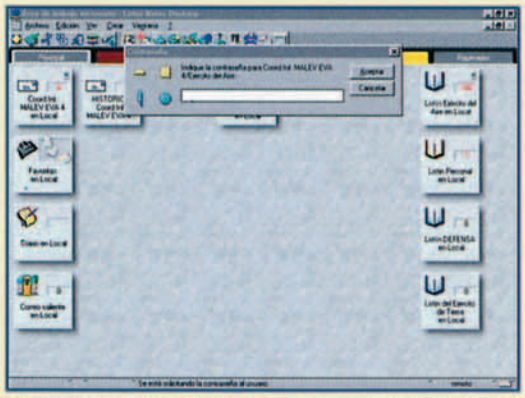
http://www.pc-shareware.com/guardian.htm
Este software permite guardar todas las contraseñas que tenemos que recordar en una base de datos...protegida por una contraseña.

http://www.geocities.com/SiliconValley/Campus/5955/index.html
O'Flaherty nos cuenta como convertirse en un "autentico" Hacker.

http://www.hedgie.com/passwords/index.html
En esta pagina se nos explican técnicas para recuperar contraseñas.

Naturalmente todas estas recomendaciones se basan en la premisa de mantener en secreto nuestra clave sin compartirla con nadie, no anotarla en ningún sitio y cambiarla frecuentemente huyendo de toda rutina o secuencia previsible. No debe ni anotarse ni usar como clave rótulos que se ofrecen a nuestra vista de forma inocente en nuestro puesto de trabajo: el letrero de un calendario, la marca del filtro de la pantalla o el titulo de un voluminoso tomo en la estantería.

Por supuesto hay que mantener también la guardia contra las técnicas para sonsacar la clave, conocidas en el argot de los 'hackers' como 'Ingeniería Social'. La primera es mirar por encima del hombro del que teclea una clave, pero otras mas atrevidas podrían ser efectuar una llamada simulando ser el administrador del sistema, el servicio técnico o un compañero en apuros que 'necesita' la clave con cualquier excusa.



En nuestro trabajo cotidiano nos vemos obligados a crear, utilizar y recordar contraseñas, de su fiabilidad como proteccion depende la seguridad de nuestros datos.

Aunque muy lejos de las fantasías mostradas por el cine, la amenaza de intrusión en sistemas informáticos con la consiguiente pérdida o divulgación de información, así como el uso ilegitimo de recursos, es un peligro real y cotidiano. Para combatirlo, todos los usuarios estamos en la primera línea de combate y debemos ser conscientes de la amenaza y tomar nuestras propias medidas. Sin ellas todas las grandes medidas que puedan adoptarse a nivel de institución pierden su efectividad, como la pierde el sistema de seguridad si al centinela de la puerta se le cuelan los extraños sin identificar.