UNIVERSIDAD TECNICA DE COTOPAXI

UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

PROYECTO DE TESIS PREVIO LA OBTENCION DEL TITULO DE INGENIERO EN INFORMATICA Y SISTEMAS COMPUTACIONALES

TEMA: **"**Investigación, análisis y pruebas de los Procesos de Esteganografía**"**

DIRECTOR: **ING. PATRICIO NAVAS MOYA**

POSTULANTES: CHICAIZA NEIRA MARCO AUGUSTO
SALAZAR MAYO SILVIA PANDORA

LATACUNGA – ECUADOR

2010

PAGINA DE RESPONSABILIDAD DE AUTORÍA

Las ideas, opiniones y comentarios en este documento son de exclusiva responsabilidad de los autores, egresados: Marco Chicaiza y Silvia Salazar

…… ……

CHICAIZA NEIRA MARCO AUGUSTO SALAZAR MAYO SILVIA PANDORA

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIDAD ACADECMICA DE CIENCIAS DE LA INGENIERIA Y APLICADAS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración.

Cumpliendo con lo estipulado en el capitulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que los postulantes: CHICAIZA NEIRA MARCO AUGUSTO y SALAZAR MAYO SILVIA PANDORA, ha desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: "**Investigación, Análisis y Pruebas de los procesos de Esteganografía para la administración de información confidencial"**, cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 19 de Abril del 2010

Atentamente,

Ing. Patricio Navas

DIRECTOR DE TESIS

AGRADECIMENTO

Al culminar esta tesis expresamos nuestro más sincero agradecimiento a la "UNIVERSIDAD TECNICA DE COTOPAXI" y a los Sres. Docentes por su valioso impulso a la formación profesional de la juventud cotopaxense,

Al Ing. Patricio Navas, asesor, quien supo guiarnos en el desarrollo de la presente tesis y a los miembros del Tribunal designado.

Silvia y Marco

DEDICATORIA

La presente tesis lo dedico con mucho cariño y amor en especial a mi hijo Kevin, a mis padres, hermanos, sobrinos, y a mi esposo, con quien compartí el aula, quienes me han impulsado para alcanzar mi objetivo.

Silvia

Este trabajo de investigación va dedicado con todo amor y cariño a mis padres que desde el cielo me guiaron y con la bendición de ellos culminado para hoy convertirme en un profesional.

Marco

ÍNDICE GENERAL

CAPITULO II

ELEMENTOS NECESARIOS PARA EL ESCOGITAMIENTO DE LOS ALGORITMOS DE ENCRIPTACION

CAPITULO III

PROPUESTA PARA LA REALIZACION DEL DESARROLLO DE LA INVESTIGACION Y PRUEBAS DEL ESTUDIO DE LA ESTEGANOGRAFIA

INTRODUCCIÓN

El mundo y la tecnología avanzan, y con ello también las técnicas de seguridad utilizadas para preservar la confidencialidad e integridad de los datos compartidos por dos o más usuarios.

Cuando utilizamos medios informáticos como el Internet, como medio de comunicación, es bastante sencillo interceptar mensajes y datos que se encuentren circulando libremente a través de las redes de computadoras y líneas telefónicas, por lo que se han ideado métodos que permitan encriptar estos mensajes y datos.

La encriptación de datos consiste en transformar los datos originales en datos no legibles para el intruso, lo que impide que este conozca el contenido de la información. Pero existe también otros métodos que permiten ocultar la información, para que los intrusos no la puedan ver, es decir, ni siquiera noten su presencia; detrás de datos legibles. El estudio de estas técnicas se conoce como “Esteganografía”, sobre la que hemos basado este proyecto de investigación con algunas citas cobre al encriptación y el criptoanálisis.

En la prensa, en libros o en la vida cotidiana hemos tenido la oportunidad de observar algunas técnicas de encriptación o de Esteganografía es así que se comenta dentro de la tesis, que los sistemas de cifra podían clasificarse de varias formas, siendo la más aceptada aquella que toma en cuenta la característica del secreto de la clave, dando lugar a criptosistemas de clave secreta y criptosistemas de clave pública. Precisamente en ello se centra el trabajo de investigación. Ahora bien, la criptología tal y como hoy en día se concibe, una técnica de enmascaramiento de la información estrechamente unida al mundo de la informática, las redes de ordenadores y las autopistas de la información, poco tiene que ver con aquella asociada a fascinantes máquinas de cifrar, que adquirieron gran fama tras su uso en la Segunda Guerra Mundial y más aún, remontándonos a siglos pasados, con los métodos, técnicas y artilugios utilizados por emperadores, gobernantes, militares y en general diversas civilizaciones para mantener sus secretos a buen recaudo.

En aquellos tiempos, el mundo de la criptología y de la esteganografía (ocultamiento de la información dentro de otra información) estaba vinculado directamente con el poder fáctico, ligado a secretos de estado, asuntos militares, de espionaje y diplomáticos, en todo caso siempre seguido de una *aureola de misterio* y que incluso salta a la literatura de ficción en el cuento "El escarabajo de oro" de Edgar Allan Poe, publicado en 1843 en "Dollar Newspaper". Se trata de un relato de aventuras cuyo eje principal gira en torno al *criptoanálisis* de un conjunto de caracteres extraños que aparecen en un pergamino cifrado y cuyo texto esconde el lugar exacto donde se encuentra enterrado el valioso tesoro de un pirata de nombre Kidd. El sistema de cifra es uno de los más simples, el denominado monoalfabético por sustitución con alfabeto mixto, de forma que el protagonista William Legrand no tiene más que aplicar las estadísticas del lenguaje, alguna que otra suposición sobre formación de palabras y una pizca de intuición para hacer corresponder los signos del enigmático criptograma con letras del alfabeto y así descriptar el mencionado pergamino.

A comienzos del siglo XX el uso de la criptografía en las transmisiones de mensajes cobra una importancia inusitada por los tiempos que corrían (Primera y Segunda Guerras Mundiales), originando esto un gran auge tanto de las técnicas como de las máquinas de cifrar. El 17 de enero de 1917 *William Montgomery*, criptoanalista de la sección diplomática de la famosa Habitación 40 del *Almirantazgo de la Marina Británica* en Londres, intercepta un telegrama lleno de códigos que el Ministro de Relaciones Exteriores alemán *Arthur Zimmermann* envía a su embajador en los Estados Unidos. Tras romper los códigos, descubren atónitos que entre otras cosas el mensaje anunciaba la guerra con los Estados Unidos. Con ello los Estados Unidos entran en la confrontación mundial y ayudan a los aliados a ganar la guerra. Según palabras de *David Khan*, autor de la obra más completa sobre historia de la criptografía, "Nunca un único criptoanálisis ha tenido tan enormes consecuencias". De hecho, el descubrimiento de este secreto cambió el rumbo de la historia. Y no es el único caso, en nuestro país de igual manera en años anteriores para los que tuvimos la suerte de leer el diario El Comercio venían unas imágenes que si se las observaba sin parpadear se podía mirar imágenes en tres dimensiones las mismas que se volvieron de moda y en todos los colegios se hacía costumbre ver que los estudiantes de aquel entonces llevaban consigo una de estas imágenes para que sus compañeros y amistades puedan descifrar el enigma.

RESUMEN

El presente trabajo de la **Investigación, Análisis y Pruebas de los procesos de Esteganografía para la administración de información confidencial** que tienen sus ventajas e inconvenientes. Su mayor utilidad radica en su simpleza. Al ser un mecanismo cuyo único fin consiste en administrar de mejor manera las contraseñas y las maneras como estas se las debe cuidar ante eventuales usuarios maliciosos que siempre tratan de violentar la información de las empresas o instituciones.

La Esteganografía es una de las técnicas que tiene poca difusión por tratarse de que todavía se encuentra en fase de difusión, y que en nuestro país lo que más se utiliza es la criptografía como método de encriptar las contraseñas que se utilizan para precautelar los servidores, las redes de información y los sistemas de forma general.

Entre los problemas que hemos podido detectar en nuestra investigación es que en nuestro país no existe la investigación hacia nuevas técnicas hasta que éstas no se encuentran probadas y que hayan sido aplicadas en otros países y que hayan tenido éxito. Esto hace que nuestro país este atrancado en cuanto al descubrimiento de nuevas tecnologías principalmente en lo que tiene que ver a este tipo de técnicas

CAPITULO I

FUNDAMENTACIÓN TEÓRICA DE LA ESTEGANOGRAFIA

1.1. INTRODUCCION

1.1.1. Sinopsis

Esteganografía: del griego "steganos" (secreto) y "grafía" (escrito). También llamada cifra encubierta Es el arte y ciencia de escribir mensajes secretos de tal forma que nadie fuera de quien lo envía y quien lo recibe sabe de su existencia, en contraste con la criptografía, en donde la existencia del mensaje es clara pero está obscurecido. Por lo general un mensaje de este tipo parece ser otra cosa, como una lista de compras, un artículo, una foto, etc. Los mensajes en la esteganografía muchas veces son cifrados primero por medios tradicionales, para posteriormente ser ocultados por ejemplo en un texto que pueda contener dicho mensaje cifrado, resultando el mensaje esteganográfico. Un texto puede ser manipulado en el tamaño de letra, espaciado, tipo y otras características para ocultar un mensaje, sólo el que lo recibe, quien sabe la técnica usada, puede extraer el mensaje y luego descifrarlo.

Por lo tanto el mundo y la Tecnología avanzan y con ello avanzan las técnicas de seguridades utilizadas para preservar la confidencialidad e integridad de los datos compartidos por dos o más usuarios.

Cuando utilizamos medios informáticos como el Internet, como medio de comunicación, es bastante sencillo interceptar mensajes y datos que se encuentren circulando libremente a través de las redes de computadoras y líneas telefónicas, por lo que se encuentren circulando libremente a y través de las redes de computadoras y líneas telefónicas, por lo que se han ideado métodos que permitan encriptar estos mensajes y datos.

La encriptación de datos consiste en "trasformar" los datos originales para el intruso, lo que impide que este conozca el contenido de la información. Pero existen también otros métodos que permiten ocultar la información, para que los intrusos no la puedan "ver", es decir, ni siquiera noten su presencia; detrás de datos legibles. El estudio de estas técnicas se conoce como "Esteganografía", sobre la cual hemos basado este proyecto.

En conclusión la Esteganografía, a diferencia de la encriptación, oculta los mensajes en datos legibles para el adversario, de tal forma que éstos pasan desapercibidos logando que el adversario nunca se entere de la existencia de estos mensajes secretos y por lo tanto no intente interceptarlos.

Cada técnica esteganográfica presenta ventajas y desventajas, pero la más apropiada es la de modificar bits menos significativos de cada píxel, para almacenar los datos. De

está forma se evita generar ruido en la imagen, y no modifica el peso de la misma; produciendo una imagen prácticamente idéntica a la original.

Cualquier técnica Esteganográfica se fortalece y se hace más eficaz, al encriptar los mensajes antes de ser ocultados en la imagen. De está forma, si es que el adversario sospecha de la existencia de mensajes ocultos en imágenes, tendría menos probabilidad de hallarlos ya que no podría diferencias entre texto encriptado y datos propios de la imagen.

1.1.2. Historia

Algunos ejemplos de técnicas de esteganografía que han sido usados en la historia son: Mensajes ocultos en tabletas de cera en la antigua Grecia (en tiempos de Herodoto), la gente escribía mensajes en una tabla de madera y después la cubrían con cera para que pareciera que no había sido usada. Existe una historia que describe como enviaron un mensaje a Esparta para avisar de que Xerxes tenía intención de invadir Gracia Mensajes secretos en papel, escritos con tintas invisibles entre líneas o en las partes en blanco de los mensajes.

Durante la segunda guerra mundial, agentes de espionaje usaban micro-puntos para mandar información, los puntos eran extremadamente pequeños comparados con los de una letra de una máquina de escribir por lo que en un punto se podía incluir todo un mensaje. Mensajes escritos en un cinturón enrollado en un bastón, de forma que sólo el diámetro adecuado revela el mensaje. Mensajes escritos en el cuero cabelludo, que tras

crecer el pelo de nuevo, oculta el mensaje. Con la llegada de los ordenadores se han ampliado y diversificado las técnicas esteganográficas.

Una de las más comunes consiste en ocultar un mensaje dentro de contenidos multimedia, mezclando los bits del mensaje original entre los bits del archivo gráfico o de sonido. El archivo resultante será una imagen o archivo de audio totalmente funcional que, a primera vista, no levanta ninguna sospecha, pero con el software adecuado es posible extraer la información oculta. Se cree que esta técnica de ocultación de mensajes fue usada por los causantes del ataque a las torres gemelas de Manhattan en Nueva York el 11 de Septiembre del 2001. Gracias a ella establecieron comunicaciones a través de Internet sobre sus futuros planes de manera sencilla y sin levantar ninguna sospecha.

Para utilizarla, se escoge un fichero, un documento Word, un documento PDF, una imagen BMP, un archivo de sonido .WAV o .MP3 que nos sirva como contenedor, y luego se crea el mensaje o el fichero que se desea ocultar. El programa que realiza la ocultación, modificará la portadora de varias formas posibles, alterando los valores de algunos de los puntos de la imagen, sumándoles o restándoles 1 (+1 para indicar el bit 1 y -1 para indicar el bit 0), de forma que sea imperceptible, pero que alguien que sepa que en esa imagen hay un mensaje, pueda recuperarlo. Otra forma de codificarlo es usar partes "no usadas" del fichero, por ejemplo, dentro de la cabecera del fichero hay a veces unos cuantos bytes que se dejan para uso de versiones posteriores, o después de la marca de fin de fichero, se puede añadir más información, sin que ningún de los programas habituales lo detecten. Existen métodos más robustos que usan tramas para el

fondo de las imágenes, o alguna modulación determinada para el sonido, y conservan el mensaje aunque se cambie de tamaño o se pase a analógico.

Esta técnica se suele usar bastante para realizar "marcas de agua", es decir, para que cuando uno vea una imagen, sepa que procede de un sitio determinado.

Uno de los programas más populares y sencillos para realizar esteganografía básica es Stego o su front-end WinStego (concretamente envían mensajes sobre texto plano). Ambos se encuentran liberados bajo la licencia GPL por tanto se consideran Software Libre. Stego está disponible para Windows y para Linux, y puede compilarse para cualquier otra plataforma. El software es español, a pesar de encontrarse en inglés.

1.1.3. Técnicas

Para poder ocultar los mensajes dentro de archivos de imagen (u otros), se utilizan distintas técnicas. Entre las más conocidas tenemos la de modificar un bit (o varios bits) de cada píxel de la imagen, generalmente los menos significativos (conocidos como LSB). La modificación de los bits nos indicaría si el mensaje (previamente convertido a binario) representa un “uno” o un “cero” en cada bit modificado de cada píxel.

Otra técnica utilizada es la de modificar píxeles completos de una imagen, pudiendo almacenar por ejemplo, un carácter en cada píxel modificado.

El problema de esta técnica es que se requiere almacenar una gran cantidad de caracteres, se generaría demasiado “ruido” en la imagen, implicando un posible comportamiento sospechoso de la misma. (Entendiendo como ruido a los píxeles que no

guardan relación en intensidad de color con los píxeles que se encuentran alrededor de éste)

Por último se puede utilizar partes no utilizadas (vacías) de un archivo para almacenar datos extras. Algunos archivos contienen una cabecera (antes de los datos del archivo en si), que contiene metadata. Es posible encontrar dentro de las cabeceras espacios vacíos que se almacenan así para su uso posterior, por lo que podemos aprovechar esos espacios vacíos para almacenar nuestros datos ocultos. Inclusive, se puede almacenar información luego del indicador de fin de archivo, pasando estos datos desapercibidos para los programas comunes de tratamiento de imágenes. El problema, obviamente se genera al agregar más bytes al archivo, con lo que se aumentaría de tamaño.

Pero no todas las técnicas de Esteganografía tienen que ver con ocultar texto en imágenes o archivos de música. Podríamos utilizar texto para ocultar texto también. Por ejemplo:

"*Arrebato de su anillo hirió dos infantes atolondrados. Arroz y pescado aseguran apetitoso omelet"*

Si extraemos la segunda letra de cada palabra, obtenemos "*reunión tres pm*", con lo que probamos una técnica esteganográfica que utiliza un texto aparentemente inofensivo y poco importante, para evitar un mensaje que, en un determinado contexto, podría definir una estrategia bélica futura.

1.2. UTLIZACION DE LAS CONTRASEÑAS

1.2.1. Aplicaciones empresariales

En criptografía, la forma de poner un password confiable es utilizando el algoritmo del **MD5** (acrónimo de *Message-Digest Algorithm 5*, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

MD5 es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (*Massachusetts Institute of Technology*, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

A pesar de su amplia difusión actual, la sucesión de problemas de seguridad detectados desde que, en 1996, Hans Dobbertin anunciase una colisión de hash plantea una serie de dudas acerca de su uso futuro.

Seguridad

A pesar de haber sido considerado criptográficamente seguro en un principio, ciertas investigaciones han revelado vulnerabilidades que hacen cuestionable el uso futuro del MD5. En agosto del 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai y Hongbo Yu anunciaron el descubrimiento de colisiones de hash para MD5. Su ataque se consumó en una hora de cálculo con un clúster IBM P690.

Aunque dicho ataque era analítico, el tamaño del *hash* (128 bits) es lo suficientemente pequeño como para que resulte vulnerable frente a ataques de 'fuerza bruta' tipo 'cumpleaños' (Ataque de cumpleaños). El proyecto de computación distribuida *MD5CRK* arrancó en marzo del 2004 con el propósito de demostrar que MD5 es

inseguro frente a uno de tales ataques, aunque acabó poco después del aviso de la publicación de la vulnerabilidad del equipo de Wang.

Debido al descubrimiento de métodos sencillos para generar colisiones de hash, muchos investigadores recomiendan su sustitución por algoritmos alternativos tales como SHA-1 o RIPEMD-160.

Aplicaciones

Los resúmenes MD5 se utilizan extensamente en el mundo del software para proporcionar la seguridad de que un archivo descargado de internet no se ha alterado. Comparando una suma MD5 publicada con la suma de comprobación del archivo descargado, un usuario puede tener la confianza suficiente de que el archivo es igual que el publicado por los desarrolladores. Esto protege al usuario contra los 'Caballos de Troya' o 'Troyanos' y virus que algún otro usuario malicioso pudiera incluir en el software. La comprobación de un archivo descargado contra su suma MD5 no detecta solamente los archivos alterados de una manera maliciosa, también reconoce una descarga corrupta o incompleta.

Para comprobar la integridad de un archivo descargado de Internet se puede utilizar una herramienta MD5 para comparar la suma MD5 de dicho archivo con un archivo MD5SUM con el resumen MD5 del primer archivo. En los sistemas UNIX, el comando de *md5sum* es un ejemplo de tal herramienta. Además, también está implementado en el lenguaje de *scripting* PHP como MD5("") entre otros.

En sistemas UNIX y GNU/Linux se utiliza el algoritmo MD5 para cifrar las claves de los usuarios. En el disco se guarda el resultado del MD5 de la clave que se introduce al dar de alta un usuario, y cuando éste quiere entrar en el sistema se compara la entrada con la que hay guardada en el disco duro, si coinciden, es la misma clave y el usuario será autenticado. He ahí el problema de encontrar y generar colisiones de *hash* a voluntad.

El MD5 también se puede usar para comprobar que los correos electrónicos no han sido alterados usando claves públicas y privadas.

1.2.2. Aplicaciones personales

Una **contraseña** o **clave** (en inglés ***password***), es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. Aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

El uso de contraseñas se remonta a la antigüedad. Centinelas que vigilaban alguna locación, requerían el santo y seña al que osara pasar. Solamente le permitían el acceso a aquella persona que conociera la contraseña. En la era moderna, las contraseñas son usadas comúnmente para controlar el acceso a sistemas operativos de computadoras protegidas, teléfonos celulares, decodificadores de TV por cable, cajeros automáticos de efectivo, etc. Un típico ordenador puede hacer uso de contraseñas para diferentes propósitos, incluyendo conexiones a cuentas de usuario, accediendo al correo

electrónico (e-mail) de los servidores, acceso a bases de datos, redes, y páginas Web, e incluso para poder leer noticias en los periódicos (diarios) electrónicos.

En la lengua inglesa se tienen dos denominaciones distintivas para las contraseñas que son: **password** (palabra de acceso) y **pass code** (código de acceso), donde la primera no implica necesariamente el uso de alguna palabra existente (sin embargo es normal el uso de alguna palabra familiar o de fácil memorización por parte del usuario), la primera suele asociarse también al uso de códigos alfanuméricos (también llamado **PIT** - *Personal Identification Text*) mientras que la segunda frecuentemente se liga al uso de algún código numérico (también llamado **PIN** - *Personal Identification Number*). Esto también ocurre en el habla española, ya que en ocasiones clave y contraseña se usan indistintamente.

Seguridad y conveniencia

En el control del acceso para todo, se realiza una relación entre seguridad y conveniencia. Es decir, si algún recurso está protegido por una contraseña, entonces la seguridad se incrementa con la consecuente pérdida de conveniencia para los usuarios. La cantidad de seguridad es inherente dada una política para contraseñas en particular que es afectada por diversos factores que se mencionarán a continuación. Sin embargo, no existe un método que sea el mejor para definir un balance apropiado entre seguridad y conveniencia.

Algunos sistemas protegidos por contraseñas plantean pocos o ningún riesgo a los usuarios si éstos se revelan, por ejemplo, una contraseña que permita el acceso a la información de una Web site gratuita. Otros plantean un modesto riesgo económico o de privacidad, por ejemplo, un **password** utilizado para acceder al **e-mail**, o alguna

contraseña para algún teléfono celular. Aún así, en otras situaciones se pueden tener consecuencias severas si la contraseña es revelada, tales como las usadas para limitar el acceso de expedientes sobre tratamientos del SIDA o el control de estaciones de energía.

Posibilidad de que algún atacante pueda adivinar o inventar la contraseña.

La posibilidad de que algún atacante pueda proporcionar una contraseña que adivino es un factor clave al determinar la seguridad de un sistema. Algunos sistemas imponen un límite de tiempo después de que un pequeño número de intentos fallidos de proporcionar la clave se dan lugar. Al no tener otras vulnerabilidades, estos sistemas pueden estar relativamente seguros con simples contraseñas, mientras éstas no sean fácilmente adivinadas, al no asignar datos fácilmente conocidos como nombres de familiares o de mascotas, el número de matrícula del automóvil o passwords sencillos como "*administrador*" o "*1234*".

Otros sistemas almacenan o transmiten una pista de la contraseña de manera que la pista puede ser fundamental para el acceso de algún atacante. Cuando esto ocurre, (y es muy común), el atacante intentara suministrar contraseñas frecuentemente en una alta proporción, quizás utilizando listas extensamente conocidas de passwords comunes. También están sujetas a un alto grado de vulnerabilidad aquellas contraseñas que se usan para generar claves criptográficas, por ejemplo, cifrado de discos, o seguridad wi-fi, por lo tanto son necesarias contraseñas más inaccesibles en estos casos.

Formas de almacenar contraseñas

Algunos sistemas almacenan contraseñas como archivos de texto. Si algún atacante gana acceso al archivo que contienen las contraseñas, entonces todas éstas se

encontraran comprometidas. Si algunos usuarios emplean el mismo password para diferentes cuentas, éstas estarán comprometidas de igual manera. Los mejores sistemas almacenan las contraseñas en una forma de protección criptográfica, así, el acceso a la contraseña será más difícil para algún espía que haya ganado el acceso interno al sistema, aunque la validación todavía sigue siendo posible.

Un esquema criptográfico común almacena solamente una forma burda de la contraseña. Cuando un usuario teclea la contraseña en este tipo de sistema, se corre a través de un algoritmo, y si el valor del valor proporcionado es igual al almacenado en la base de datos de contraseñas, se permite el acceso al usuario.

El valor burdo de la contraseña se crea al aplicar una función criptográfica para secuenciar la consistencia del password y, normalmente, otro valor conocido como salt. La salt previene que los atacantes construyan una lista de valores para contraseñas comunes. Las funciones criptográficas más comunes son la MD5 y SHA1. Una versión modificada de DES fue utilizada en los primeros sistemas Unix.

Si la función que almacena el password está bien diseñada, no es computacionalmente factible revertirla para encontrar el texto directamente. Sin embargo, si algún atacante gana acceso a los valores (y muchos sistemas no los protegen adecuadamente), puede usar gran cantidad de herramientas disponibles para comparar los resultados cifrados de cada palabra dentro de una colección, como un diccionario. Están ampliamente disponibles largas listas de contraseñas posibles en muchos lenguajes y las herramientas intentarán diferentes variaciones. Estas herramientas demuestran con su existencia la relativa fortaleza de las diferentes opciones de contraseña en contra de ataques. El uso derivado de una función para una clave puede reducir este riesgo.

Desafortunadamente, existe un conflicto fundamental entre el uso de estas funciones y la necesidad de un reto de autenticación; este último requiere que ambas partes se pueden una a otra para conocer el secreto compartido (es decir, la contraseña), y al hacer esto, el servidor necesita ser capaz de obtener el secreto compartido en su forma almacenada. En los sistemas Unix al hacer una autenticación remota, el secreto compartido se convierte en la forma burda de la contraseña, no la contraseña en sí misma; si un atacante puede obtener una copia de la forma burda de la contraseña, entonces será capaz de acceder al sistema remotamente, incluso sin tener que determinar cuál fue la contraseña original.

Método de retransmisión de la contraseña al usuario

Las contraseñas pueden ser vulnerables al espionaje mientras son transmitidas a la máquina de autenticación o al usuario. Si la contraseña es llevada como señal eléctrica sobre un cableado no asegurado entre el punto de acceso del usuario y el sistema central que controla la base de datos de la contraseña, está sujeta a espionaje por medio de métodos de conexiones externas en el cableado. Si ésta es enviada por medio de Internet, cualquier persona capaz de ver los paquetes de información que contienen la información de acceso puede espiar el password con pocas posibilidades de detección. Los cable módem pueden ser más vulnerables al espionaje que DSL los módems y las conexiones telefónicas, el ethernet puede estar o no sujeto a espionaje, dependiendo particularmente de la opción del hardware de la red y del cableado. Algunas organizaciones han notado un incremento significativo de las cuentas robadas después de que los usuarios se conecten por medio de conexiones por cable.

El riesgo de intercepción de los password mandados por Internet pueden ser reducidos con una capa de transporte de seguridad (TLS - Transport Layer Security, previamente

llamada SSL) que se integra en muchos navegadores de Internet. La mayoría de los navegadores muestran un icono de un candado cerrado cuando el TLS está en uso. Vea criptografía para otras maneras en las que pasar la información puede ser más seguro.

Procedimientos para cambiar las contraseñas

Usualmente, un sistema debe proveer una manera de cambiar un password, ya sea porque el usuario sospeche que el password actual ha (o ha sido) descubierto, o como medida de precaución. Si el nuevo password es introducido en el sistema de una manera no cifrada, la seguridad puede haberse perdido incluso antes de que el nuevo password haya sido instalado en la base de datos. Si el nuevo password fue revelado a un empleado de confianza, se gana poco. Algunos web sites incluyen la opción de recordar el password de un usuario de una manera no cifrada al mandárselo por e-mail.

Los **Sistemas de Administración de Identidad**, se utilizan cada vez más para automatizar la emisión de reemplazos para contraseñas perdidas. La identidad del usuario se verifica al realizar algunas preguntas y compararlas con las que se tienen almacenadas. Preguntas típicas incluyen las siguientes: "¿Dónde naciste?", "¿Cuál es tu película favorita?", "¿Cuál es el nombre de tu mascota?" En muchos casos las respuestas a estas preguntas pueden ser adivinadas, determinadas con un poco de investigación, u obtenidas a través de estafa con ingeniería social. Mientras que muchos usuarios han sido advertidos para que nunca revelen su password, muy pocos consideran el nombre de su película favorita para requerir este tipo de seguridad.

1.2.3. Aplicaciones Bancarias (ATM: Cajeros Automáticos)

El sistema de video vigilancia ATM-INTELLECT se diseña para tener control 24/7 sobre cajeros automáticos. Todos los eventos que tienen lugar en un cajero automático

durante las horas de operación, son grabados y almacenados en las bases de datos. Este sistema previene de pérdidas financieras causadas por fraude y vandalismo.

Las tareas del sistema son:

- Reducción de las pérdidas financieras relacionadas con actividades fraudulentas al retirar dinero de los cajeros automáticos;
- Reducción de pérdidas financieras bancarias causadas por actos de vandalismo en cajeros automáticos;
- Asegurar que los requerimientos de seguridad, en las operaciones y mantenimiento en cajeros automáticos son observados;

La administración y control centralizados, aseguran una monitorización de todos los cajeros automáticos. Almacena y procesa datos, notifica operaciones de situaciones de emergencia e instantáneamente, transmite la señal de alarma mediante imágenes a través del servicio de seguridad. La imagen del área alrededor de los cajeros automáticos se muestra al operador a través de una pantalla, así como la zona de recepción del dinero y la localización del cajero automático. Todos los eventos acaecidos en operaciones en los cajeros automáticos son archivados en la base de datos. Si es necesario, el archivo de video es analizado. (Por ejemplo si el poseedor de una tarjeta hace reclamaciones injustificadas a la entidad bancaria):

- Por número de tarjeta;
- Por día y hora;
- Por evento.

El ATM-INTELLECT asegura la ejecución de las siguientes funciones:

- Video grabación;
- Grabación continua;
- Grabación mediante la activación del detector de actividad;
- Grabación bajo el disparo de sensores (sensor por vibración, sensor de apertura de puertas, sensor de temperatura, sensor de fuego e intrusión);
- Muestra los datos del vídeo;
- Muestra los datos del vídeo en el centro de seguridad;
- Recibos, procesamiento y grabación de mensajes provenientes del ordenador central de cajeros automáticos;
- Transmisión de señales de alarma bajo la apariencia de situaciones de emergencia en las operaciones de los cajeros automáticos;
- Búsqueda de archivos de vídeo, preparación de informes y transmisión de los resultados de búsqueda;
- Monitorización de las condiciones técnicas;
- Transmisión de los mensajes de alarma y de imágenes de vídeo al centro de control de los cajeros automáticos a través de la red mediante los canales regulares X.85 y TCP/IP;
- Revisión simultánea de varias cámaras.

1.3. TENDENCIAS DE LA ENCRIPTACION

1.3.1. Definiciones

Encriptar es la codificación de los datos por razones de seguridad. Los sitios comerciales en la red previenen que las personas no autorizadas vean información

confidencial como los números de tarjeta de crédito, que se envían desde y hacia sus sitios. La codificación se hace mediante un proceso que se conoce como encripción, que manejan algoritmos sofisticados que solo pueden ser interpretados por servidores Web y visores de Internet que soporten el mismo protocolo de encripción.

La encriptación requiere que el mismo protocolo se utilice en ambos lados para poder codificar en el lado emisor y decodificar en el lado receptor. La decodificación no significa que pueda ser entendida por un humano. Por ejemplo, en una transacción electrónica de pago con tarjeta de crédito, el número de la tarjeta solo lo ve la persona que lo digita. El resto de la información viaja encriptada desde el portal de compra, al banco, y de vuelta al portal de compra con un mensaje de Aprobación o negación.

1.3.2. Unificación de los sistemas

En todos los sistemas operativos el cifrado o encriptación de los passwords es un tópico no muy usual. Aunque es importante distinguir si hablamos de passwords encriptadas o no encriptadas, lo que realmente marca la diferencia es el método de encriptación que se utiliza. Esto es debido a que muchas veces, lo que nos parece un fichero encriptado es, simplemente, un fichero "codificado". Esto hace que para nosotros el fichero no sea leíble directamente, pero si que lo podríamos entender o traducir fácilmente usando un ordenador.

Además, incluso un fichero encriptado podría haber sido generado mediante una clave débil (fácil de adivinar) o un esquema de encriptación poco robusto.

Por estas razones es importante que, en el caso de encriptar cualquier tipo de información, seas consciente de que estas usando un esquema de encriptación confiable el cual ha sido probado y verificado a fondo. Por otro lado, debes asegurarte de que tu password es también un password robusto. Un buen sistema de encriptación no sirve de nada sin un buen password. Y viceversa.

1.3.3. La razón y su importancia

La importancia de tener un password en un sistema o archivo de información es la de precautelar su integridad.

Un password robusto es aquél que:

- No puede encontrarse en un diccionario
- Contiene números, letras y símbolos
- Contiene letras mayúsculas y minúsculas
- Cuanto más largo, más robusto es.

Con un password de 2 letras y 26 letras en el alfabeto, contando además con 10 números (ignorando los símbolos), hay 236 posibles combinaciones (687,000,000 posibilidades). Si aumentamos la longitud del password a 8 caracteres, ya disponemos de 836 combinaciones (324,000,000,000,000,000,000,000,000,000,000 posibilidades).

Hay muchos generadores de passwords robustos disponibles en Internet, pero éstos generarán un password que es casi imposible de recordar.

Intente emplear, en cambio, una cadena aparentemente aleatoria de letras o números que usted pueda recordar fácilmente.

Por ejemplo:

Ys=#1pt! (Yo soy el numero uno para ti)

ArJuAg1p (Ariadna, Juan Agustín y 1 perro – miembros de la familia)

LxRzDg24 (Alex Ruiz Diego – consonantes del nombre completo y la edad)

1.3.4. Tecnología de Encriptación

Toda encriptación se encuentra basada en un Algoritmo, la función de este Algoritmo es básicamente codificar la información para que sea indescifrable a simple vista , de manera que una letra *"A"* pueda equivaler a :*"5x5mBwE" o bien a "xQE9fq"*, el trabajo del algoritmo es precisamente determinar como será transformada la información de su estado original a otro que sea muy difícil de descifrar.

Una vez que la información arrive a su destino final, se aplica el algoritmo al contenido codificado *"5x5mBwE" o bien a "xQE9fq"* y resulta en la letra *"A"* o según sea el caso, en otra letra. Hoy en día los algoritmos de encriptación son ampliamente conocidos,es por esto que para prevenir a otro usuario "no autorizado" descifrar información encriptada, el algoritmo utiliza lo que es denominado **llave ("key")** para controlar la encriptación y decriptación de información. Algunos algoritmos son DES (algoritmo

simétrico) AES que posiblemente suplantará a **DES** y uno de los más conocidos RSA (algoritmo asimétrico)

Función de la llave ("key")

Existen dos tipos de llaves ("key's") , pero la de mayor uso en Internet es denominada "public key" o algoritmo asimétrico. El nombre "public" proviene de su funcionamiento: existe una llave pública que es dada a conocer a cualquier persona que así lo desee (todo Internet), esta llave pública es utilizada por los emisores de mensajes para encriptar información , sin embargo, existe otra llave (su pareja por llamarla de alguna manera) *única* que es conocida *exclusivamente* por el destinatario del mensaje, y es mediante esta llave *única* | *secreta* que el destinatario descifra ("decripta") los mensajes encriptados por el emisor.

Firmas Digitales ("Digital Signatures")

Una **firma digital** utiliza el mismo funcionamiento del "public key" o algoritmo asimétrico mencionado anteriormente.

Como se mencionó, existe una "llave pública" y una "llave secreta", en el caso de **firmas digitales** la llave pública que es ampliamente conocida es capaz de identificar si la información proviene de una fuente fidedigna.En otras palabras, la llave pública será capaz de reconocer si la información realmente proviene de la "llave secreta" en cuestión. Ejemplo:

El departamento de compras posee las *llaves públicas* de todos los empleados de la compañía, si llega un pedimento con la dirección de email del Director de Finanzas, Cómo puede asegurarse el departamento de compras que en realidad esta persona realizó el pedimento y no alguna otra que sobrepuso el email ?. La *llave secreta* del director de finanzas debe de encontrarse solo en su computadora, por lo tanto al enviar el mensaje electrónico esta *llave pública* se añadió al email,y por lo tanto las *llave publicas* determinarán si la *llave secreta* coincide con la del director.

1.4. VULNERABILIDADES

Password Cracking (password Recovery)

El Password Cracking o el descifrado de contraseñas para propósitos ilegales es, evidentemente, ilegal. Pero si es su propio password el que quiere descifrar, entonces estamos hablando de su información. Si de lo que se trata es de que un individuo está utilizando un password para proteger algo, y entonces se olvida de éste, se necesita una recuperación de contraseña o password recovery.

El descubrimiento de passwords consiste en seguir unas técnicas básicas:

- Echar una mirada alrededor: los passwords se guardan a menudo debajo de los teclados, bajo las alfombrillas del ratón o se cuelgan en las hojas "*post-it*" personales.

- La fuerza bruta: simplemente se prueban passwords de forma secuencial hasta que uno funciona.

- Los ataques de diccionario automatizados: estos programas cruzan una serie de palabras pertenecientes a un diccionario hasta que una de éstas funcione como una contraseña válida.

Hay muchos programas disponibles en Internet que nos pueden ayudar con la recuperación de passwords introducidos en diferentes tipos de documentos. Sin embargo, cuanta más nueva es la versión del programa más fiable éste se vuelve y, por consiguiente, más difícil es obtener los passwords descifrados que usan, o encontrar un programa que nos ayude en la recuperación del password.

El uso de contraseñas se remonta a la antigüedad: los centinelas que vigilaban una posición solicitaban el «santo y seña» al que quisiera pasar. Solamente le permiten el acceso a aquella persona que conoce la seña. En la era tecnológica, las contraseñas son usadas comúnmente para controlar el acceso a sistemas operativos de computadoras protegidas, teléfonos celulares, decodificadores de TV por cable, cajeros automáticos de efectivo, etc. Un típico ordenador puede hacer uso de contraseñas para diferentes propósitos, incluyendo conexiones a cuentas de usuario, accediendo al correo electrónico (e-mail) de los servidores, accediendo a bases de datos, redes, y páginas Web, e incluso para leer noticias en los periódicos (diarios) electrónicos.

En la lengua inglesa se tienen dos denominaciones distintivas para las contraseñas: **password** (palabra de acceso) y **pass code** (código de acceso), donde la primera no implica necesariamente usar alguna palabra existente (sin embargo, es normal emplear alguna palabra familiar o de fácil memorización por parte del usuario), la primera suele asociarse también al uso de códigos alfanuméricos (también

llamado **PIT** - *Personal Identification Text*), mientras que la segunda frecuentemente se liga a la utilización de algún código numérico (asimismo llamado **PIN** - *Personal Identification Number*). Esto ocurre igualmente en el habla española, ya que en ocasiones clave y contraseña se usan indistintamente.

Para el control de acceso total, se realiza una relación entre seguridad y comodidad para evitar que alguien extraño tenga acceso a ciertos recursos. Es decir, si algún recurso está protegido por una contraseña, entonces la seguridad se incrementa con el consecuente aumento de molestia para los usuarios. El nivel de seguridad es inherente dada una política de contraseñas en particular, que está influida por diversos factores que se mencionarán a continuación. Sin embargo, no existe un método único que sea el mejor para definir un balance adecuado entre seguridad y comodidad de acceso.

Algunos sistemas protegidos por contraseñas plantean pocos o ningún riesgo a los usuarios si éstos se revelan, por ejemplo, una contraseña que permita el acceso a la información de una Web site gratuita. Otros plantean un modesto riesgo económico o de privacidad, por ejemplo, una **contraseña** utilizada para acceder al **e-mail**, o alguna contraseña para algún teléfono celular. Aún así, en otras situaciones, puede tener consecuencias severas, si la contraseña es revelada. Por ejemplo, como las situaciones para limitar el acceso de expedientes sobre tratamientos del SIDA o el control de estaciones de energía.

La posibilidad de que algún atacante pueda proporcionar una contraseña que adivinó es un factor clave al determinar la seguridad de un sistema. Algunos sistemas imponen un límite de tiempo después de que sucede un pequeño número de intentos fallidos de proporcionar la clave. Al no tener otras vulnerabilidades, estos sistemas pueden estar relativamente seguros con simples contraseñas, mientras estas no sean fácilmente deducibles, al no asignar datos fácilmente conocidos como nombres de familiares o de mascotas, el número de matrícula del automóvil o contraseñas sencillas como "*administrador*" o "*1234*".

Otros sistemas almacenan o transmiten una pista a modo de sugerencia de recordatorio de la contraseña, de manera que la propia pista puede ser fundamental para el acceso de algún atacante. Cuando esto ocurre, (y suele ser común), el atacante intentará suministrar contraseñas frecuentemente en una alta proporción, quizás utilizando listas extensamente conocidas de contraseñas comunes. También están sujetas a un alto grado de vulnerabilidad aquellas contraseñas que se usan para generar claves criptográficas, por ejemplo, cifrado de discos, o seguridad wi-fi, por lo tanto son necesarias contraseñas más inaccesibles en estos casos.

Formas de almacenar contraseñas

Algunos sistemas almacenan contraseñas como archivos de texto. Si algún atacante gana acceso al archivo que contienen las contraseñas, entonces todas éstas se encontrarán comprometidas. Si algunos usuarios emplean la misma contraseña para diferentes cuentas, éstas estarán comprometidas de igual manera. Los mejores sistemas almacenan las contraseñas en una forma de protección criptográfica, así, el acceso a la contraseña será más difícil para algún espía que haya ganado el acceso interno al sistema, aunque la validación todavía sigue siendo posible.

Un esquema criptográfico común almacena solamente el texto de la contraseña codificado, conocido como *hash*. Cuando un usuario teclea la contraseña en este tipo de sistema, se genera a partir de la contraseña y mediante un algoritmo el código hash equivalente para esa contraseña, y si el resultante (hash) coincide con el valor almacenado, se permite el acceso al usuario.

El texto codificado de la contraseña se crea al aplicar una función criptográfica usando la contraseña y normalmente, otro valor conocido como *salt* en inglés. El *salt* previene que los atacantes construyan una lista de valores para contraseñas comunes. Las funciones criptográficas más comunes son la MD5 y SHA1. Una versión modificada de DES fue utilizada en los primeros sistemas Unix.

Si la función que almacena la contraseña está bien diseñada, no es computacionalmente factible revertirla para encontrar el texto directamente. Sin embargo, si algún atacante gana acceso a los valores (y muchos sistemas no los protegen adecuadamente), puede usar gran cantidad de herramientas disponibles para comparar los resultados cifrados de cada palabra dentro de una colección, como un diccionario. Están ampliamente disponibles largas listas de contraseñas posibles en muchos lenguajes y las herramientas intentarán diferentes variaciones. Estas herramientas demuestran con su existencia la relativa fortaleza de las diferentes opciones de contraseña en contra de ataques. El uso derivado de una función para una clave puede reducir este riesgo.

Desafortunadamente, existe un conflicto fundamental entre el uso de estas funciones y la necesidad de un reto de autenticación; este último requiere que ambas partes se pueden una a otra para conocer el secreto compartido (es decir, la contraseña), y al hacer esto, el servidor necesita ser capaz de obtener el secreto compartido en su forma almacenada. En los sistemas Unix al hacer una autenticación remota, el secreto compartido se convierte en la forma burda de la contraseña, no la contraseña en sí misma; si un atacante puede obtener una copia de la forma burda de la contraseña, entonces será capaz de acceder al sistema remotamente, incluso sin tener que determinar cuál fue la contraseña original.

Método de retransmisión de la contraseña al usuario

Las contraseñas pueden ser vulnerables al espionaje mientras son transmitidas a la máquina de autenticación o al usuario. Si la contraseña es llevada como señal eléctrica sobre un cableado no asegurado entre el punto de acceso del usuario y el sistema central que controla la base de datos de la contraseña, está sujeta a espionaje por medio de métodos de conexiones externas en el cableado. Si ésta es enviada por medio de Internet, cualquier persona capaz de ver los paquetes de información que contienen la información de acceso puede espiar la contraseña con pocas posibilidades de detección.

Los cable módem pueden ser más vulnerables al espionaje que DSL los módems y las conexiones telefónicas, el ethernet puede estar o no sujeto a espionaje, dependiendo particularmente de la opción del hardware de la red y del cableado. Algunas organizaciones han notado un incremento significativo de las cuentas robadas después de que los usuarios se conecten por medio de conexiones por cable.

El riesgo de intercepción de las contraseña mandadas por Internet pueden ser reducidos con una capa de transporte de seguridad (TLS - Transport Layer Security, previamente llamada SSL) que se integra en muchos navegadores de Internet. La mayoría de los navegadores muestran un icono de un candado cerrado cuando el TLS está en uso. Vea criptografía para otras maneras en las que pasar la información puede ser más seguro.

Procedimientos para cambiar las contraseñas

Usualmente, un sistema debe proveer una manera de cambiar una contraseña, ya sea porque el usuario sospeche que la contraseña actual ha (o ha sido) descubierto, o como medida de precaución. Si la nueva contraseña es introducida en el sistema de una manera no cifrada, la seguridad puede haberse perdido incluso antes de que la nueva contraseña haya sido instalada en la base de datos. Si la nueva contraseña fue revelada a un empleado de confianza, se gana poco. Algunos web sites incluyen la opción de recordar la contraseña de un usuario de una manera no cifrada al mandárselo por e-mail.

Los **Sistemas de Administración de Identidad**, se utilizan cada vez más para automatizar la emisión de reemplazos para contraseñas perdidas. La identidad del usuario se verifica al realizar algunas preguntas y compararlas con las que se tienen almacenadas. Preguntas típicas incluyen las siguientes: "¿Dónde naciste?", "¿Cuál es tu película favorita?", "¿Cuál es el nombre de tu mascota?" En muchos casos las respuestas a estas preguntas pueden ser adivinadas, determinadas con un poco de investigación, u obtenidas a través de estafa coningeniería social. Mientras que muchos usuarios han sido advertidos para que nunca revelen su contraseña, muy pocos consideran el nombre de su película favorita para requerir este tipo de seguridad.

Longevidad de una contraseña

El forzar a los usuarios a que cambien su contraseña frecuentemente (ya sea semestralmente, mensualmente o en lapsos más frecuentes) asegura que una contraseña válida en manos equivocadas sea eventualmente inútil. Muchos sistemas operativos proveen esta opción, aunque ésta no se usa universalmente. Los beneficios de seguridad son limitados debido a que los atacantes frecuentemente sacan provecho de una contraseña tan pronto como ésta es revelada. En muchos casos, particularmente con las cuentas de administradores o cuentas "raíz", una vez que un cracker ha ganado acceso, puede realizar alteraciones al sistema operativo que le permitirán accesos futuros incluso si la contraseña inicial ya ha expirado.

Forzar cambios de contraseña frecuentemente hace que los usuarios tiendan a olvidar cual es la contraseña actual, y por esto se da la consecuente tentación de escribir las claves en lugares a la vista o que reutilicen contraseñas anteriores, lo cual niega cualquier beneficio de seguridad. Al implementar este tipo de política se requiere una cuidadosa consideración de los factores humanos.

Número de usuarios por cada contraseña

En algunas ocasiones, una sola contraseña controla el acceso de un dispositivo, por ejemplo, para la red de un router, o para un teléfono móvil. Sin embargo, en el caso de un sistema informático, una contraseña se almacena generalmente para cada nombre de usuario, de este modo haciendo que todos los accesos puedan ser detectables (excepto, por supuesto, en el caso de usuarios que comparten la misma contraseña).

En estos casos, un usuario potencial debe proporcionar un nombre y una contraseña. Si el usuario provee una contraseña que coincide con el almacenado para el nombre de usuario, entonces se le permite el acceso al sistema del ordenador. Este también es el caso de los cajeros automáticos, con la excepción de que el nombre de usuario es el

número de cuenta almacenado en la tarjeta del cliente, y que el PIN es normalmente muy corto (de 4 a 6 dígitos).

La asignación de contraseñas separadas a cada usuario de un sistema es normalmente preferible que hacer que una sola contraseña sea compartida por varios usuarios legítimos del sistema. Esto se da en parte porque la gente está más dispuesta a revelar a otra persona (quién no puede estar autorizada) una contraseña compartida que era exclusivamente para su propio uso. Contraseñas individuales para cada usuario también son esenciales si los usuarios son responsables por sus actividades, tales como en los casos de transacciones financieras o consulta de expedientes médicos.

Diseño de software protegido

Técnicas comunes utilizadas para mejorar la seguridad de sistemas de software protegidas por contraseñas incluyen:

- No repetir la contraseña en la pantalla de visualización cuando se está accediendo.
- Permitir contraseñas de una longitud adecuada (algunos sistemas de Unix limitan contraseñas a 8 caracteres)
- Obligar a que la contraseña tenga algún carácter especial y algún número
- Requerir a los usuarios volver a ingresar su contraseña después de un período de inactividad.
- Hacer cumplir una política de contraseñas para asegurar contraseñas importantes.
- Requerir periódicamente cambios de contraseña.
- Asignar contraseñas al azar.
- Proveer una opción alternativa al uso de teclados.
- Al cambiar la contraseña, comprobar que no se parece a las contraseñas anteriormente usadas.
- Las medidas más rigurosas corren un riesgo de enajenar a usuarios.

Probabilidad que una contraseña pueda ser descubierta [editar]

Estudios en la producción de sistemas informáticos han indicado por décadas constantemente que cerca de 40% de las contraseñas elegidas por usuarios se conjeturan fácilmente.

- Muchos de los usuarios no cambian la contraseña que viene predeterminada en muchos de los sistemas de seguridad. Las listas de estas contraseñas están disponibles en el Internet.

- Una contraseña puede ser determinada si un usuario elige como contraseña un dato personal que sea fácil de descubrir (por ejemplo: el número de ID o el número de cuenta de un estudiante, el nombre del novio/a, la fecha de cumpleaños, el número telefónico, etc.). Los datos personales sobre individuos están ahora disponibles en diferentes fuentes, muchas de ellas están en línea, y pueden obtenerse frecuentemente por alguien que use técnicas de ingeniería social, como actuar como un trabajador social que realiza encuestas.

- Una contraseña es vulnerable si puede encontrarse en una lista. Los diccionarios (frecuentemente de forma electrónica) están disponibles en muchos lenguajes, y existen listas de contraseñas comunes.

- En pruebas sobre sistemas en vivo, los ataques de diccionarios son rutinariamente acertados, por lo que el software implementado en este tipo de ataques ya se encuentra disponible para muchos sistemas. Una contraseña muy corta, quizás elegida por conveniencia, es más vulnerable si un hacker puede obtener la versión criptográfica de la contraseña. Las computadoras son en la actualidad lo suficientemente rápidas para intentar todas las contraseñas en orden alfabético que tengan menos de 7 caracteres, por ejemplo:

Una **contraseña débil** sería una que fuese muy corta o que fuese la predeterminada, o una que pudiera adivinarse rápidamente al buscar una serie de palabras que es posible encontrar en diccionarios, nombres propios, palabras basadas en variaciones del nombre del usuario. Una contraseña fuerte debe ser suficientemente larga, al azar, o producirse

sólo por el usuario que la eligió, de modo tal que el 'adivinarla' requiera un largo tiempo. Ese tiempo 'demasiado largo' variará de acuerdo al atacante, sus recursos, la facilidad con la que la contraseña se pueda descubrir, y la importancia de ésta para el atacante. Por lo tanto, una contraseña de un estudiante quizás no valga la pena para invertir más de algunos segundos en la computadora, mientras que la contraseña para acceder al control de una transferencia de dinero del sistema de un banco puede valer varias semanas de trabajo en una computadora.

'Fuerte' y 'débil' tienen significado solamente con respecto a tentativas de descubrir la contraseña de un usuario, ya sea por una persona que conoce al usuario, o una computadora que trate de usar millones de combinaciones. En este contexto, los términos pueden tener una precisión considerable. Pero nótese que una contraseña 'fuerte' en este sentido puede ser robada, truqueada o extraída del usuario ya sea mediante la extracción del historial de un teclado, grabada mediante aparatos de comunicación o copiada de notas dejadas por olvido.

Ejemplos de contraseñas débiles incluyen las siguientes: *administrador, 1234*, "nombre del usuario", xx/xx/xx - fechas importantes, ya que la mayoría de estas se encuentran en bases de datos o en diccionarios (dictionary search attack). Ejemplos de contraseñas fuertes serían las siguientes: *tastywheeT34, partei@34!* y *#23kLLflux*. Estas contraseñas son largas y usan combinaciones de letras mayúsculas y minúsculas, de números y de símbolos. No pueden hallarse fácilmente en listas de contraseñas y son suficientemente largas para provocar que una búsqueda burda resulte impráctica en la mayor parte de los casos. Nótese que algunos sistemas no permiten símbolos como #, @ y ! en contraseñas y son más difíciles de encontrar en algunos teclados diseñados para ciertos países. En estos casos, agregar uno o dos caracteres (letra o número) puede ofrecer una seguridad equivalente. También es importante observar que, a partir de la publicación en Internet de este texto que está usted leyendo, estos ejemplos específicos de contraseñas ya no resultarán buenas opciones: ejemplos de discusiones públicas sobre contraseñas obviamente son buenos candidatos para incluirse en las listas de diccionarios para atacar sistemas.

El método más efectivo para generar contraseñas es seleccionar suficientes caracteres al azar, aunque este tipo de contraseñas son las más difíciles de recordar. Algunos usuarios desarrollan frases o palabras compuestas que tienen letras al azar como iniciales de varias palabras. Otra manera de elaborar contraseñas al azar que sean más memorables es usar palabras al azar o sílabas en lugar de letras al azar.

En ocasiones se recomienda el uso de recuerdos personales, es decir, elementos o datos que sean memorables para una persona en particular pero no para otras. Por ejemplo: la contraseña *yt21cvpppv* es difícil de recordar, pero se deriva de la frase "Yo tenía 21 cuando visité París por primera vez", posiblemente muy fácil de recordar para el usuario que vivió esa experiencia. Sin embargo, si la primera visita a Paris fue un hecho muy trascendente para un usuario en particular, es posible que otra persona que conozca a ese usuario y sepa de la importancia que para él tuvo ese viaje pueda adivinar más o menos fácilmente la contraseña y, por lo tanto, ésta no sería una opción sensata para utilizarse como contraseña.

Probabilidad de que una contraseña pueda ser recordada

Las contraseñas más seguras son largas, y con caracteres al azar. Con un mismo número de caracteres, la contraseña será más fuerte (ofrecerá mayor seguridad al usuario) si incluye una mezcla de mayúsculas y minúsculas, números y otros símbolos (cuando es posible utilizar estos últimos). Desafortunadamente, desde la perspectiva de seguridad, estos tipos de contraseña son los más difíciles de recordar.

El forzar a los usuarios a utilizar contraseñas creadas 'al azar' por el sistema asegura que la contraseña no tendrá conexión con el usuario y, por lo tanto, no podrá ser encontrada en ningún diccionario. Varios sistemas operativos incluyen esta opción. Aunque es provechoso desde el punto de vista de seguridad, muchos usuarios evitan tales medidas y la cooperación del usuario es generalmente esencial para un sistema de seguridad.

Los usuarios de computadoras suelen recibir la advertencia en el sentido de que "nunca deben escribir la contraseña en ninguna parte, sin excepción" y de que "nunca deben usar la contraseña para más de una cuenta". Estas declaraciones, aunque suenan bien en teoría, ignoran la realidad de que un usuario de computadoras puede tener docenas de cuentas protegidas por contraseña. Tienen la consecuencia involuntaria de que muchos usuarios seleccionan contraseñas débiles, incluso para cuentas importantes, y terminan por utilizar la misma contraseña en todas ellas.

Si el usuario escribe las contraseñas en algún lugar para poder recordarlas posteriormente, no deberá guardarlas en lugares obvios (agendas, debajo de los teclados, al reverso de las fotografías, etc.). La peor ubicación (y, sin embargo, la más común) es en una nota pegada en la computadora. Las cajas con candado para objetos valiosos son una mejor opción para el resguardo de información importante como las contraseñas. Existe software disponible para computadoras portables (palm, computadoras portátiles muy pequeñas) que almacenan las contraseñas de numerosas cuentas de manera cifrada. Otra opción puede ser elegir una sola contraseña para cuentas de poca importancia, y elegir contraseñas más rigurosas para un menor número de aplicaciones relevantes como las cuentas de banco en línea.

En una conferencia de seguridad en 2005, un experto de Microsoft declaró: "*Creo que la política sobre contraseñas debería decir que ustedes deban escribir sus contraseñas en algún lugar para recordarlas posteriormente. Yo tengo 68 contraseñas diferentes. Si no se me permite escribirlas en algún lugar, ¿adivinen que es lo que voy a hacer? Voy a usar la misma contraseña en cada unas de mis cuentas*."

¿Qué es más desventajoso? ¿Usar contraseñas débiles fáciles o usar contraseñas fuertes pero escritas en algún lugar visible? Este dilema puede provocar un gran debate entre los expertos. La seguridad práctica requiere a menudo alcanzar un equilibrio entre los requisitos de conflicto y los factores humanos.

Probabilidad de que una contraseña sea descubierta

Las contraseñas pueden ser descubiertas mediante navegación en la red, robo, extorsión, allanamiento, amenazas u otros métodos. La búsqueda en los contenedores de basura ha resultado ser fructífera en situaciones donde se desechan datos importantes sin suficiente precaución (como se ha probado recientemente con el reciente robo de identidades). El número de caracteres de una contraseña no sólo puede ser determinado al espiar la pantalla del usuario, sino también al contar el número de clicks al teclear una contraseña. Una investigación publicada por IBM en 2004 muestra que cada tecla de un teclado tiene un sonido distintivo, lo que permite tonalizar datos, incluidas las contraseñas, para que puedan ser recuperadas al analizar grabaciones de un dispositivo de sonido o *bug* (véase Criptoanálisis acústico).

El obtener contraseñas mediante manipulación psicológica de los usuarios es un ejemplo de ingeniería social. Un atacante puede telefonear a un usuario y decir: "Hola, le hablamos de Control de Sistemas. Estamos haciendo una prueba de seguridad. ¿Puede proporcionarme su contraseña para que podamos proceder?" Los administradores de sistema y demás personal de soporte técnico casi nunca necesitan conocer la contraseña de un usuario para poder realizar sus trabajos. Los administradores de sistema con privilegios de "raíz" o incluso sus superiores pueden cambiar las contraseñas de los usuarios sin su permiso, así que no tienen necesidad de requerirlas. Además, éstos evitarán pedir las contraseñas, precisamente porque no desean crear el hábito de revelar las contraseñas a cualquiera.

Las numerosas maneras en las que las contraseñas reusables pueden comprometer la seguridad han impulsado el desarrollo de otras técnicas. Desafortunadamente, ninguna se ha vuelto tan disponible universalmente para los usuarios que buscan una alternativa más segura.

- Contraseñas de un solo uso: Tener contraseñas que solamente son válidas en una ocasión hace que los ataques potenciales resulten ineficaces. Para la mayoría de los usuarios las contraseñas de un solo uso resultan extremadamente inconvenientes y,

ello no obstante, éstas se han implementado ampliamente en la banca personal en línea, donde se les conoce como TANs. Ya que la mayoría de los usuarios sólo realizan un pequeño número de transacciones cada semana, el uso de contraseñas de un solo uso no ha generado insatisfacción en los usuarios en estos casos.

- Símbolos de seguridad: Son similares a las contraseñas de un solo uso, pero el valor que debe ingresarse aparece en un pequeño F.O.B., y éste cambia cada minuto.

- Controles de acceso: Se basan en la criptografía pública dominante, es decir, SSH. Las claves necesarias son demasiado grandes para memorizar y deben almacenarse en una computadora local, en un símbolo de seguridad o en un dispositivo de memoria portable, como por ejemplo en una memoria flash o en un disco flexible.

- Métodos biométricos: Permiten la personalización basándose en características personales inalterables, aunque en la actualidad tienen altas tasas de error y requieren hardware adicional para escaneo de rasgos corporales (por ejemplo, las huellas digitales, el iris ocular, etc.).

CAPITULO II

2. ELEMENTOS NECESARIOS PARA EL ESCOGITAMIENTO DE LOS ALGORITMOS DE ENCRIPTACION

2.1. Parámetros a tomar en cuenta para la asignación de contraseñas a nivel de servidores

Para la administración adecuada en proporcionar contraseñas seguras hay que tomar en cuenta mucho los parámetros que sugieren los desarrolladores de las distintas plataformas, siendo esto muy importante al momento de asignar privilegios de acuerdo a las funciones que desempeñan las personas que accederán a los sistemas o a las plataformas

Así tenemos que para el sistema operativo de Windows el 2003 Server de la empresa Microsoft el formato para poder asignar contraseñas se sigue el siguiente formato o los pasos que a continuación detallamos:

Inicio de Sesión interactiva: La cual confirma la identidad del usuario en el computador local o en el Directorio Activo (Active Directory AD).

- Autentificación de Red: La cual confirma la identidad de usuario para cualquier recurso que intente acceder. Para proveer autentificación de red w2k3 utiliza cuatro mecanismos los cuales son:
    - Kerberos V5
    - Autenticación (SSL/TLS)
    - NTLM
    - Certificados de llave publica
- Paralelamente con la autentificación del usuario, w2k3 permite que los administradores controlen el acceso a los recursos, o los objetos, en la red.
- w2k3 implementa el control de acceso mediante descriptores (access control list ACL) por los cuales asignan seguridad a los objetos almacenados en directorio activo.

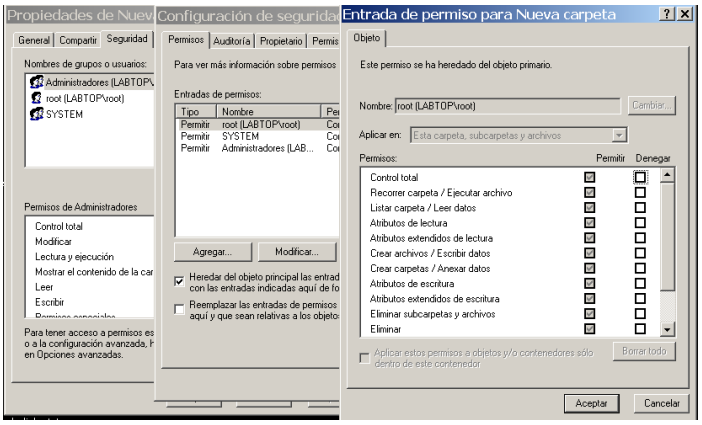


Gráfico 2.1: Instancia donde asigna usuarios y privilegios en Windows 2003

Fuente: Los Investigadores

El directorio activo proporciona el almacenaje protegido de la cuenta del usuario y de la información del grupo usando control de acceso en objetos y credenciales del usuario. Debido a esto el directorio activo no solamente almacena credenciales del usuario sino también la información del control de acceso, los usuarios que entran a la red obtienen la autentificación y la autorización de tener acceso a recursos de sistema (discretionary access control list DACL) .

Adicionalmente a la autentificación y control de acceso, existen otros aspectos importantes del modelo de seguridad de w2k3, los cuales son: Políticas de seguridad, auditoría, Protección de datos, Infraestructura de llave pública.

Desde Windows 2003 en adelante todos los sistemas operativos que llevan la característica de NT(Nueva Tecnología), son capaces de cifrar todas las contraseñas que se van a ingresar, en los servidores y los clientes siempre y cuando estén validados en el Active Directory.

SISTEMA DE CIFRADO

Sistema de cifrado (Encrypting File System EFS)

- Se cifra usando el algoritmo 3DES y el Archivo de llave de cifrado (File Encryption Key FEK) generada aleatoriamente.
- FEK cifra utilizando la clave publica del usuario FEK solo puede ser descifrado con la llave privada del usuario
- Cada archivo tiene su propio FEK

- El campo Data Decryption Field (DDF) mantiene el FEK cifrada con la llave publica del usuario

No se necesita descifrar el archivos antes de ser usado (trasparente)

- Reside en el Kernel
- Soporta cifrado remoto de archivos remotos
- Los archivos puede ser cifrados mediante el explorador o mediante el "cipher" en la línea de comandos

No se pueden cifrar archivos o carpetas comprimidas

- Los archivos de sistema no se pueden cifrar
- Los archivos cifrados se pueden borrar
- Los directorios cifrados no cifran la lista de archivos contenidos
- La opción de cifrado de un directorio cifra todos los archivos contenidos en el
- Si se copia un directorio cifrado a un sistema de archivos no NTFS este no queda cifrado

Cuando un usuario cifra un archivo, se genera un FEK y se usa DES-X para cifrar el archivo mediante FEK

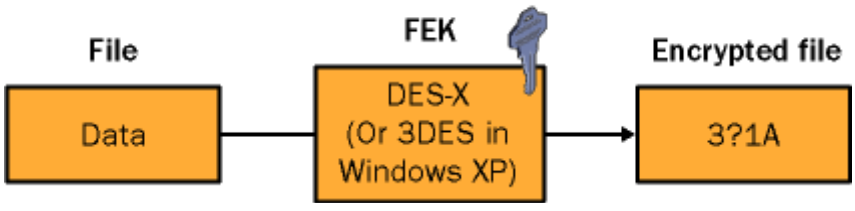


Gráfico 2.2: Forma de Encriptación Windows 2003 y Windows XP

l

Fuente: Los Investigadores

A continuación se recupera la llave pública del certificado de EFS del perfil de usuario. La FEK se cifra utilizando el algoritmo RSA y la clave publica del certificado EFS del usuario y se agrega al encabezado del archivo en el campo de descifrado de datos (Data Decryption Field DDF)

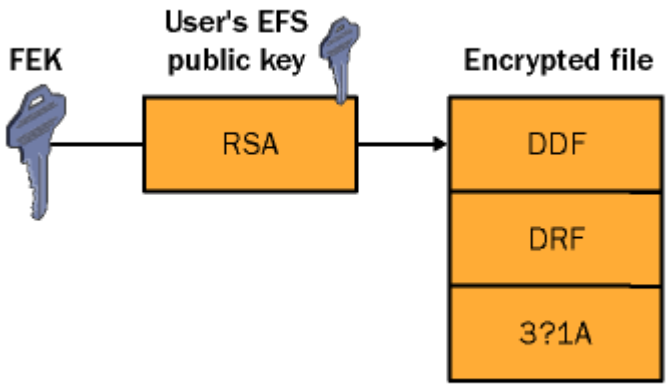


Gráfico 2.3: Archivos de Encriptación

Fuente: Los Investigadores

Pueden descifrar los datos cifrados por los usuarios

- Solo la FEK está disponible para los agentes. (no la llave privada del usuario)
- Los administradores locales son los agentes recuperadores por omisión en las computadoras stand alone

- Los administradores de domino son los agentes recuperadores por omisión para el domino

La política de los agentes recuperadores de datos se define en el controlador de domino.

- Las políticas se aplican a las computadoras (no a los usuarios)
- No hay acumulación de esta política.

PRINCIPIOS DE SEGURIDADES EN LINUX

El sistema operativo Linux en sus distintas versiones lo que siempre a precautelado es la seguridad de la información misma que se genera al momento de almacenar la información en sus sistemas de ficheros.

Una norma básica de seguridad radica en la asignación a cada usuario sólo de los permisos necesarios para poder cubrir las necesidades de su trabajo sin poner en riesgo el trabajo de los demás.

Riesgos

- Dentro del sistema Linux todo son archivos: desde la memoria física del equipo hasta el ratón, pasando por módems, teclado, impresoras etc.
- Esta filosofía de diseño es uno de los factores que mas éxito y potencia proporciona a Linux, pero también uno de los que mas peligros, debido a

que un simple error en un permiso puede permitir a un usuario modificar todo el disco duro, o leer los datos tecleados desde una Terminal etc.

- El sistema de archivos es la parte del núcleo (Kernel) mas visible por los usuarios; se encarga de abstraer propiedades físicas de los diferentes dispositivos para proporcionar una interfaz única de almacenamiento: el archivo.

- Cada sistema Linux tiene su sistema de archivos nativo. (ejemplo ext3)
- Un primer criterio para mantener un sistema seguro es una correcta distribución del espacio de almacenamiento.

- Esto limita el riesgo de que el deterioro de una partición afecte a todo el sistema. La pérdida se limitaría al contenido de esa partición
- Tamaño de las particiones
- No hay unas normas generales aplicables; el uso al que vaya destinado el sistema y la experiencia son las bases de la decisión adecuada, aunque por lo general se recomienda:

- Si el sistema va a dar servicio a múltiples usuarios que requieren almacenamiento para sus datos es conveniente que el directorio /home tenga su propia partición.
- Si el equipo va a ser un servidor el directorio /var o incluso /var/spool deberían tener su propia partición.
- Debe dimensionar cuidadosamente la partición raíz.
- El directorio /usr/local contiene los programas compilados e instalados por el administrador. Resulta conveniente usar una partición propia para

proteger estos programas personalizados de futuras actualizaciones del sistema. Este criterio también se puede aplicar al directorio /opt

Los permisos de cada archivo son la protección mas básica de estos objetos del sistema operativo; definen quien puede acceder a cada uno de ellos, y de que forma puede hacerlo. Cuando hacemos un ls -l podemos ver sus permisos junto al tipo de archivo correspondiente, en la primera columna de cada línea:

user:~# ls -l texto.txt

-rw-r--r--1 user electric 512 Aug 3 2009 texto.txt

Propiedad:

- Qué usuario y grupo posee el control de los permisos del i-nodo. Se almacenan como dos valores numéricos, el uid (user id) y gid (group id).

Permisos:

- Bits individuales que definen el acceso a un Archivo o directorio. Los permisos para directorio tienen un sentido diferente a los permisos para Archivos. Más abajo se explican algunas diferencias

Lectura (r):

- **Archivo**: Poder acceder a los contenidos de un Archivo
- **Directorio**: Poder leer un directorio, ver qué Archivos contiene

Escritura (w):

- **Archivo**: Poder modificar o añadir contenido a un Archivo
- **Directorio**: Poder borrar o mover Archivos en un directorio

Ejecución(x):

- **Archivo**: Poder ejecutar un programa binario o guión de shell
- **Directorio**: Poder entrar en un directorio

Cifrado de archivos:

- GnuPG: Gnu Privacy Guard
- TCFS: Transparent Cryptographic File System
  - Cryptographic File System CFS
- TrueCrypt

Casi todas las actividades realizadas en un sistema Linux son susceptibles a ser monitorizadas: desde las horas de acceso de cada usuario al sistema hasta las páginas web más frecuentemente visitadas, pasando por los intentos fallidos de conexión, los programas ejecutados o incluso el tiempo de CPU que cada usuario consume.

Es evidente que esta facilidad para recolectar información tiene grandes ventajas para la seguridad: ya que es posible detectar un intento de ataque nada mas con producirse el mismo, así como también es posible detectar usos indebidos de los recursos del sistema o actividades **sospechosas**; sin embargo, existen también una gran desventajas, ya que la gran cantidad de información que

potencialmente se registra puede ser aprovechada para crear ataques de negaciones de servicio o, más habitualmente, la cantidad de información recopilada puede dificultar el detectar problemas por el volumen de datos a analizar.

El demonio syslogd

- El demonio syslogd es el encargado de recolectar los datos de los eventos del sistema y demás actividades dependiendo de su archivo de configuración (/etc/syslogd.conf).
- Los logs creados por el syslogd son comúnmente usado por los IDS-Host
- Los archivos de salida del syslogd son en texto plano lo cual facilita su visualización
- Los archivo de logs se encuentran por lo general en /var/logs/
- Todas las entradas que presenta syslogd tienen como mínimo una fecha y una hora, el nombre de la maquina y del programa que generó el evento.
- Existen diferentes tipos de archivos de log dependiendo de la información. Por ejemplo, existe un archivo de log del sistema, un archivo de log para los mensajes de seguridad y un archivo de log para las tareas cron.
- Los logs del sistema deben ser rotados periódicamente para poder disminuir su tamaño
- Los logs pueden ser comprimidos

- Los parámetros y la cantidad de logs que se guardan en el sistema dependerán en parte de la capacidad de los discos duros.
- **/var/log/syslog:**es el archivo de log más importante del sistema; en el se guardan mensajes relativos a la seguridad de la maquina, como los accesos o los intentos de acceso a ciertos servicios. No obstante, este archivo es escrito por syslogd, por lo que dependiendo de nuestro archivo de configuración encontraremos en el archivo una u otra información
- **/var/log/messages :** En este archivo se almacenan datos `informativos' de ciertos programas, mensajes de baja o media prioridad destinados mas a informar que a avisar de sucesos importantes, como información relativa al arranque de la maquina.

Inetd

- En las primeras versiones de Unix, para hacer funcionar un servicio de red se ejecutaban programas diferentes que atendían a cada uno. Al crecer el número de servicios que se necesitaban, se optó por una mejor idea, se empezó a utilizar un sólo demonio llamado */etc/inetd*(El daemon de Internet). Este programa escuchaba en varios puertos a la vez y ejecutaba los servidores que se necesitaran en el momento en que se recibía la petición de conexión.
- Inetd se ejecuta cuando la máquina arranca, formando parte del proceso de arranque mismo. Cuando empieza su ejecución revisa el archivo de configuración */etc/inetd.conf*para determinar qué servicios de red debe controlar

- Cuando un host cliente intenta conectarse a un servicio de red controlado por inetd, el súper servicio recibe la petición y verifica por cualquier regla de control de acceso wrappers TCP.

- Si se permite el acceso, inetd verifica que la conexión sea permitida bajo sus propias reglas para ese servicio y que el servicio no esté consumiendo más de la cantidad de recursos o si está rompiendo alguna regla. Luego comienza una instancia del servicio solicitado y pasa el control de la conexión al mismo.

- Una vez establecida la conexión, inetd no interfieremás con la comunicación entre el host cliente y el servidor
- El wrappers TCP proporciona control de acceso basado en host a los servicios de red. El componente más importante dentro del paquete es la librería /usr/lib/libwrap.a. En términos generales, un servicio wrappers TCP es uno que ha sido compilado con la librería libwrap.a.
- Cuando un intento de conexión es hecho a un servicio wrapped TCP, el servicio primero referencia los archivos de *acceso de host*(/etc/hosts.allow y /etc/hosts.deny) para determinar si el cliente tiene permitido conectarse. Luego utiliza el demonio syslog (syslogd) para escribir el nombre del host solicitante y el servicio solicitado a /var/log/secure o /var/log/messages.
- Si a un cliente se le permite conectarse, los TCP wrappers liberan el control de la conexión al servicio solicitado y no interfieren más con la comunicación entre el cliente y el servidor.

- Además del control de acceso y registro, los TCP wrappers pueden activar comandos para interactuar con el cliente antes de negar o liberar el control de la conexión al servicio solicitado.
- Puesto que los TCP wrappers son una utilidad de gran valor a las herramientas de seguridad de cualquier administrador de servidor. Algunas de los demonio que utilizan TCP wrappers son /usr/sbin/sshd, /usr/sbin/sendmail, y /usr/sbin/inetd.

2.2 Parámetros a tomar en cuenta para la asignación de contraseñas a nivel de computadores personales

Para poder ingresar a una red cualquiera sea la configuración de esta debemos tener en cuenta las políticas del servidor de dominios el mismo que asigna privilegios de acuerdo a las necesidades de cada uno de los usuarios del sistema.

Gráfico 2.4: Archivos de Encriptación

Fuente: Los Investigadores

El ingreso de las contraseñas con que cuentan los clientes que están equipados con Windows XP se los hace validando en el Active Directory del Windows 2003 en

el caso de la plataforma de Microsoft como se puedo observar en paginas anteriores de este mismo trabajo investigativo, de la misma manera se requiere de un usuario que fue creado en el directorio /hoem de la raíz del Linux y esto sucede en cualquiera de las opciones con que cuenta este difundido sistema operativo, así mismo puede hacérselo en las plataformas de Solaris y AS400 de IB; las mismas que básicamente fueron armadas a través de Unix como es el caso de Linux.

2.3 Logros o insuficiencias observadas en el sistema actual de asignación de contraseñas.

Para poder determinar los aciertos y desaciertos del sistema actual a manera de verificar la criptografía como paso previo al estudio a fondo de la esteganográfica podemos mencionar que existe muchos software en la red los mismos que ayudan a descencriptar los archivos tal es el caso que los hackers utilizan muchos de estos software para determinar primero que nada cuales son los puertos que se encuentran abiertos para luego proceder a ingresar y poder hacer el daño que se requiera.

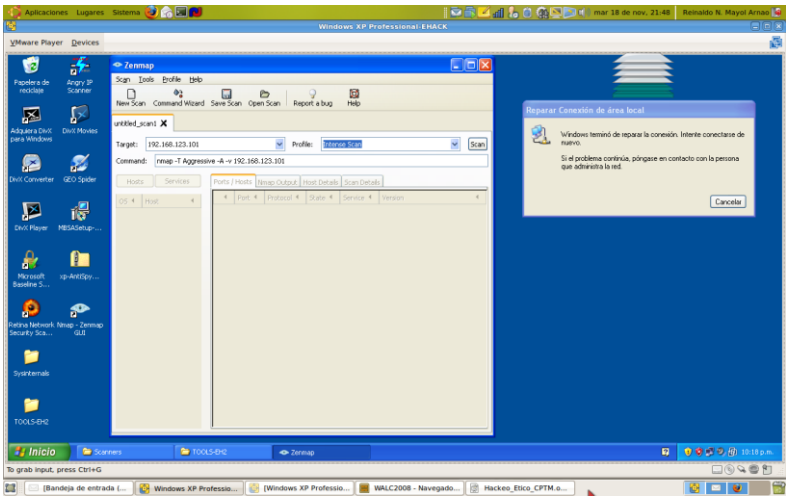


Gráfico 2.5: Software para rastrear puertos abiertos

Fuente: www.softdownload.com

En este caso podemos observar esta aplicación que se encuentra de forma gratuita en el internet trabaja buscando puertos abiertos en el servidor y luego los archivos que pueden ayudar a la descifrar las contraseñas que se encuentran almacenadas para poder acceder a la información que aquí se encuentra guardada.

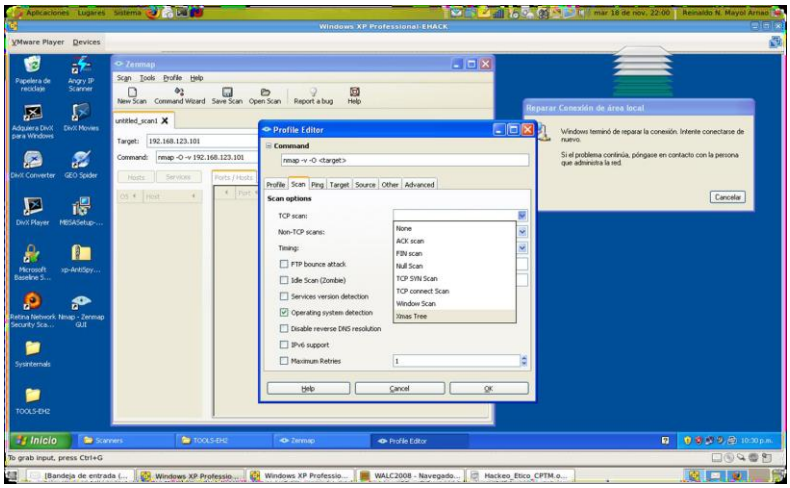


Gráfico 2.6: Software para rastrear puertos abiertos

Fuente: www.softdownload.com

Una vez que se rastreo al 100%, nos emite un reporte que nos indica el sistema operativo al cual escaneo, los puertos que se encuentran abiertos es necesario hacer notar que solo trabaja con puertos que tengan el protocolo TCP/IP ya que este es el encargado de interpretar las señales que puede emitir el NMAP.

2.4 Logros o insuficiencias observadas en el Internet.

Algo que ha causado siempre gran misterio es sin lugar a dudas el cómo trabajan los hackers y crackers los mismos que son capaces de causar gran daño a instituciones que cuentan con una gran infraestructura tecnológica y que son en algunos casos los descubridores de nuevas fuentes de investigación a nivel de seguridades en todo sea este en software o hardware.

Así tenemos un ejemplo de lo que le sucedió a la página web de la ONU(Organización de las Naciones Unidas), la misma que fue visitada por los hackers como se puede observar en el siguiente grafico.

Gráfico 2.7: Pagina web de la ONU Crackeada

Fuente: www.opensecurity.es

Entonces nuevamente nace la discusión si será seguro subir los negocios al internet en lo que ya se conoce como el comercio electrónico e-business, ya que si paginas de organizaciones que no persiguen fines de lucro son invadidas, las paginas que tienen que ver con fines comerciales y bancarias son blancos frecuentes de este tipo de personas que se escudan en la investigación de nuevas formas de hacer daño.

El grafico siguiente fue expuesto en un congreso de programadores de páginas web que se desarrollo en la ciudad de México en el año 2008.

Gráfico 2.8: Porque son comprometidas las Paginas web

Fuente: Coloquio Internacional de Programadores WEB Mexico-2008

- Obtención de identidades mediante ataques de "hombre en el medio".
- Envenenamiento del Cache del DNS.
- Explotando errores de los programas.
- Explotando configuraciones incorrectas.
- Envenenamiento de URL
- Inyecciones SQL
- DoS(Ataques de Sistema)

Resumiendo y dando interpretación a los cuatro fundamentales problemas que se encuentran en el plano podemos mencionar lo anteriormente citado

2.5 Entrevistas con personal administrativo y docentes de la Carrea de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi conocedores del tema

Al tratarse que la criptografía y por ende la esteganográfica son temas nuevos nuestra investigación se lo realizado tanto a docentes como al personal de la dirección de servicios informáticos y las respuestas fueron de lo más variado.

Las entrevistas que se lo realizaron fueron plateadas a nivel de conocimiento y de aplicabilidad tanto en la parte académica como en la parte administrativa ya que si se conoce o no de la esteganográfica fue de las primeras inquietudes a nivel de docencia la gran parte de docentes entrevistados nos manifestaron que algunas veces se ha escuchado este tipo de términos y que se encuentra relacionado con la criptografía que es muy cierto pero no del todo ya que la una en cripta de manera de que no pueda ser legible en cambio la otra lo hace para poder poner un anzuelo a los usuarios de computadores que desean ingresar a los computadores o servidores de la empresas con el fin de poder husmear en la información que generen las empresas.

Si se aplica este tipo de conocimiento en la parte académica todavía no se lo realiza ya que no existe fuente bibliográfica suficiente para poder realizar trabajos con este tipo de técnicas.

En el caso del personal que labora en la dirección de servicios informáticos de igual manera tiene nociones de que es la esteganográfica pero no se conoce a ciencia cierta de que se trata o como puede ser aplicado, se profundizo un tanto más con nuestro tema y se nos manifestó que el sistema escolástico contaba con 4 formas de seguridad de la información que se genera en esta aplicación ya que se lo hace a través de los servidores de dos formas diferentes mediante firewall y mediante los permisos a usuarios que brinda el Active directory del Windows 2003 R2 que es el que almacena la aplicación.

La aplicación cuenta con un algoritmo de encriptación de contraseñas la misma que se basó fundamentalmente en el MD5, de igual manera se filtro a través de los números de cedula de las personas que ingresan al sistema tales como Administradores, docentes, administrativos, y estudiantes en general que son los usuarios más frecuentes de esta aplicación.

Es necesario contar con bibliografía suficiente de este tipo de temas en las bibliotecas principalmente de la Universidad ya que la esteganografia es una de las herramientas con las que cuenta el departamento de defensa de ls estados Unidos de América para precautelar la información que ellos generan, es importante mencionar de igual manera que la esteganografía nació de un estudio desarrollado en las Fuerzas Armadas Americanas con el fin de blindar la información que se generaba en sus portaaviones que eran desplazados hacia Oriente Medio para las distintos conflictos armados que allá tenían.

2.6 Análisis de las entrevistas planteadas

Como se puede observar en el siguiente cuadro:

ENTREVISTAS REALIZADAS AL PERSONAL DE LA UNIVERSIDAD TECNICA DE COTOPAXI		
1	PERSONAL ADMINISTRATIVO	4
2	PERSONAL DOCENTE	6
3	ESTUDIANTES 8vo. CICLO	12
	SUMAN	22

Cuadro 2.1. Personal Entrevistado
Fuente: Grupo Investigador

Para la mayoría de las personas entrevistadas este tipo de temas resulta relativamente nuevos sobre todo al preguntarse como Esteganografía no asi se el tema a tratarse es la criptografía o el ocultamiento de la información ya que de este tipo de temas se tiene un amplio concepto.

La encriptación de contraseñas mediante algoritmos fue de lo mas común ya que muchos de los entrevistados manifestaron que cuando desarrollan software el algoritmo preferido es el MD5 que como se vio en nuestro análisis ya no es 100% utilizado por que ya había sido alterado de parte de los hackers.

El personal que se entrevisto en la Dirección de Servicios Informáticos nos manifestaba que para servidores de Proxy y seguridad se utilizaban las claves de ocultamiento que proporciona Microsoft a través de Windows 2003, no ha si el Escolástico el mismo que fue diseñado un algoritmo en C# pero que tiene mucho que ver con lo que es el MD5.

2.7 Comprobación de la Hipótesis

En Nuestro plan de estudio se había plateado como hipótesis lo siguiente: El desarrollo de una Investigación sustentada en varios estudios de diversas técnicas de Esteganografía garantizaría la seguridad de las contraseñas en los servidores y computadores personales.

Se ha podido establecer a lo largo de esta investigación muchas formas de encriptar contraseñas pero sobre todo se trata de ayudar a que cuando en el diario convivir no puedan ser víctimas de asaltos o de robos de contraseñas para la utilización de cajeros automáticos.

La esteganografía ya no es una utopía sino que se la está palpando a diario con la forma como se esconde la información en archivos, textos, imágenes, archivos de música, en fin en material que todos los días manipulamos.

Es importante de igual manera tomar en cuenta mucho las alternativas que se plantean en este documento de cómo se puede interpretar de mejor manera la información oculta, de que se quiere esconder, cual es el beneficio de disfrazar la información

Con estas pautas que se plantean en este trabajo de investigación se concluye que la hipótesis planteada está bien sustentada.

CAPITULO III

3. PROPUESTA PARA LA REALIZACIÓN DEL DESARROLLO DE LA INVESTIGACION Y PRUEBAS DEL ESTUDIO DE LA ESTEGANOGRAFIA.

3.1. Introducción

La esteganografía proporciona los medios para ocultar la existencia y presencia de los datos lo que permite proteger dichos datos de posible monitorización no autorizada y no deseada. Aparte de la esteganografía existen otros métodos complementarios para conseguir la confidencialidad de datos secretos: Cifrado. Es el proceso de transformar los datos o texto en claro utilizando operaciones matemáticas a una forma alternativa de los datos originales denominado texto cifrado. Los datos cifrados sólo pueden ser entendidos por las partes autorizadas que dispongan de las claves para descifrar el texto cifrado o criptograma en el texto en claro original. El cifrado no oculta la existencia de los datos lo que oculta es su contenido, es decir el significado de los datos. Ocultar directorios

en Windows. Windows permite a los usuarios ocultar ficheros. Utilizando esta característica es fácil cambiar las propiedades de un directorio para ocultarlo, de este modo, el usuario no autorizado no podrá ver todos los tipos de ficheros con su explorador. Ocultar directorios en Unix. Sobre directorios existentes que dispongan de un gran conjunto de ficheros, como en el directorio /dev en una implementación Unix, consiste en hacer que un directorio comience con tres puntos (…) en vez de utilizar normalmente un punto o dos puntos. Canales encubiertos-subliminares. Algunas herramientas se pueden utilizar para transmitir datos valiosos sobre un tráfico de red aparentemente normal. Una de dichas herramientas es Loki que oculta los datos secretos sobre tráfico ICMP (como ping). La esteganografía permite colocar la información secreta en carriers (soportes aparentemente inofensivos y que pueden pasar de-sapercibidos) muy diversos tales como imágenes, ficheros de audio, ficheros de video, ficheros de texto, espacio de disco, particiones ocultas en discos, paquetes que circulan en tráfico de red (normalmente en las cabeceras de las PDUs), en software, en circuitería hardware.

Existen muy diversas técnicas a través de las cuales la esteganografía permite ocultar información secreta, pueden clasificarse en:

Métodos de sustitución. Consiste en sustituir bits del carrier o tapadera no sospechosa por los bits del mensaje a ocultar. Posibles técnicas: métodos bit-plane y métodos basados en la paleta de colores. Los métodos bit-plane utilizan como carrier por ejemplo imágenes, consiste en reemplazar el LSB (Least Significant Bit) de la intensidad de la imagen con los bits del mensaje, se sustituye 1, 2, 3 o 4 LSB con los bits del mensaje secreto o datos de imagen a ocultar. Los datos se ocultan como ruido de la imagen. De este modo se pueden ocultar grandes cantidades de datos. Se trata éste de un método muy frágil ante posibles manipulaciones de la imagen resultante que oculta la información secreta en el carrier. Variaciones de los métodos bit-plane consiste en utilizar una permutación de localizaciones de los píxel en las que se ocultan los bits, bien empleando generadores de números pseudoaleatorios o PRNG cuyo módulo es el tamaño de la imagen (número píxeles). Los métodos basados en paleta de colores se basan en cambiar el color o paleta de escala de grises que

representa los colores de la imagen. El método basado en la inserción del bit menos significativo es el más común y popular y consiste en hacer uso del LSB de la información de píxel de la imagen. De este modo la distorsión global se mantiene al mínimo mientras el mensaje se espacia sobre los píxeles de la imagen. Esta técnica opera mejor cuando el fichero de imagen es mayor que el mensaje secreto y si la imagen es en escala de grises.

Métodos basados en el procesamiento de señales. Por ejemplo métodos basados en transformaciones como Fourier, Wavelets, DCT, etc. y basados en espectro extendido. Estos métodos también denominados métodos basados en algoritmos y transformaciones ocultan los datos utilizando funciones matemáticas que se utilizan en algoritmos de compresión. La idea de este método es ocultar el mensaje secreto en los bits de datos de los coeficientes menos significativos.

Métodos de codificación. Por ejemplo cuantización, códigos de corrección de errores, dithering, etc.

Métodos estadísticos. Se basan en utilizar los test de hipótesis.

Métodos de generación del carrier. Por ejemplo basados en fractales y caos.

Métodos de enmascaramiento y filtrado. La información se oculta dentro de una imagen utilizando DWM (Digital WaterMarking) se incluye información como derechos de copia, propiedad o licencias. El propósito es diferente al de la esteganografía tradicional ya que consiste en añadir un atributo a la imagen de tapadera o carrier de este modo se extiende la cantidad de información presentada.

3.2. Objetivos

- Conocer cómo opera este sistema de seguridad en la teoría.
- Lograr analizar y entender las prácticas de la esteganografía.
- Discutir ventajas y desventajas
- Estudio de la seguridad de la esteganografía.

3.3. Diseño y Factibilidades de Implementación de Procesos de Esteganografía

El objetivo principal del proyecto es mostrar la existencia de un método de camuflaje de información muy útil y sencilla.

Esteganografía: del griego "steganos" (secreto) y "grafía" (escrito). También llamada cifra encubierta

Es el arte y ciencia de escribir mensajes secretos de tal forma que nadie fuera de quien lo envía y quien lo recibe sabe de su existencia, en contraste con la criptografía, en donde la existencia del mensaje es clara pero está obscurecido. Por lo general un mensaje de este tipo parece ser otra cosa, como una lista de compras, un artículo, una foto, etc.

Los mensajes en la esteganografía muchas veces son cifrados primero por medios tradicionales, para posteriormente ser ocultados por ejemplo en un texto que pueda contener dicho mensaje cifrado, resultando el mensaje esteganográfico. Un texto puede ser manipulado en el tamaño de letra, espaciado, tipo y otras características para ocultar un mensaje, sólo el que lo recibe, quien sabe la técnica usada, puede extraer el mensaje y luego descifrarlo.
Algunos ejemplos de técnicas de esteganografía que han sido usados en la historia son:

Mensajes ocultos en tabletas de cera en la antigua Grecia (en tiempos de Herodoto), la gente escribía mensajes en una tabla de madera y después la cubrían con cera para que pareciera que no había sido usada. Existe una historia que describe como enviaron un mensaje a Esparta para avisar de que Xerxes tenía intención de invadir Gracia Mensajes secretos en papel, escritos con tintas invisibles entre líneas o en las partes en blanco de los mensajes.

Durante la segunda guerra mundial, agentes de espionaje usaban micro-puntos para mandar información, los puntos eran extremadamente pequeños comparados con los de una letra de una máquina de escribir por lo que en un punto se podía incluir todo un mensaje.

Mensajes escritos en un cinturón enrollado en un bastón, de forma que sólo el diámetro adecuado revela el mensaje.

Mensajes escritos en el cuero cabelludo, que tras crecer el pelo de nuevo, oculta el mensaje.

Con la llegada de los ordenadores se han ampliado y diversificado las técnicas esteganográficas.

Una de las más comunes consiste en ocultar un mensaje dentro de contenidos multimedia, mezclando los bits del mensaje original entre los bits del archivo gráfico o de sonido. El archivo resultante será una imagen o archivo de audio totalmente funcional que, a primera vista, no levanta ninguna sospecha, pero con el software adecuado es posible extraer la información oculta.

Se cree que esta técnica de ocultación de mensajes fue usada por los causantes del ataque a las torres gemelas de Manhattan en Nueva York el 11 de Septiembre del 2001. Gracias a ella establecieron comunicaciones a través de Internet sobre sus futuros planes de manera sencilla y sin levantar ninguna sospecha.

Para utilizarla, se escoge un fichero, un documento Word, un documento PDF, una imagen BMP, un archivo de sonido .WAV o .MP3 que nos sirva como contenedor, y luego se crea el mensaje o el fichero que se desea ocultar. El programa que realiza la ocultación, modificará la portadora de varias formas posibles, alterando los valores de algunos de los puntos de la imagen, sumándoles o restándoles 1 (+1 para indicar el bit 1 y -1 para indicar el bit 0), de forma que sea imperceptible, pero que alguien que sepa que en esa imagen hay un mensaje, pueda recuperarlo.

Otra forma de codificarlo es usar partes "no usadas" del fichero, por ejemplo, dentro de la cabecera del fichero hay a veces unos cuantos bytes que se dejan para uso de versiones posteriores, o después de la marca de fin de fichero, se puede añadir más información, sin que ningún de los programas habituales lo detecten. Existen métodos más robustos que usan tramas para el fondo de las imágenes, o alguna modulación determinada para el sonido, y conservan el mensaje aunque se cambie de tamaño o se pase a analógico.

Esta técnica se suele usar bastante para realizar "marcas de agua", es decir, para que cuando uno vea una imagen, sepa que procede de un sitio determinado.

Uno de los programas más populares y sencillos para realizar esteganografía básica es Stego o su front-end WinStego (concretamente envían mensajes sobre texto plano). Ambos se encuentran liberados bajo la licencia GPL por tanto se consideran Software Libre. Stego está disponible para Windows y para Linux, y puede compilarse para cualquier otra plataforma. El software es español, a pesar de encontrarse en inglés.

3.3.1. Factibilidad Técnica

Para la aplicación de esta técnica se debe tomar en cuenta muchos aspectos entre los cuales podemos destacar las metodologías de la

encriptación y de la ocultación de la información en símbolos nueros o en las mismas letras.

Métodos

Métodos clásicos

La esteganografía da sus primeros pasos en la antigua Grecia. Se cuenta en "*Les Històries d'Heròdot*" que Demeratus quería comunicar a la ciudad de Esparta que Xerxes tenía planes para invadir Grecia. Para evitar ser capturado por espionaje en los controles, escribió sus mensajes en tablas que luego fueron cubiertas con cera, de forma que parecían no haber sido usadas.

Ésta es posiblemente una de las primeras manifestaciones en la historia de mensajes esteganografiados.

Otro método usado durante siglos consistía en tatuar al mensajero (generalmente un esclavo) un mensaje en la cabeza afeitada para después dejarle crecer el pelo y enviar así el mensaje oculto.
Un ejemplo de método clásico es el siguiente:
Tesis de Sistemas
Uftjt0ef0tjtufnbt
Vguku1fg1ukuvgocu
Whvlv2gh2vlvwhpdv

En ese ejemplo podemos mirar cómo se podría encriptar una frase como Tesis de Sistemas, y solamente con cuatro idiomas y sin necesidad de recurrir ni a gráficos ni algoritmos difíciles de descifrar.

Cifrado nulo (Null Cipher)

El método de escritura de meta-información en un texto es usado desde hace siglos, y sigue siendo usado hoy en día. Esto es debido a que se trata posiblemente de uno de los métodos más sencillos de ocultar información.

Consiste en escribir un texto aparentemente inofensivo donde, mediante algún mecanismo conocido por el legítimo receptor de la información (actualmente hablamos de algoritmos y claves), subyace la información realmente importante.

Para la aplicación de la factibilidad operacional miremos un ejemplo de un espía alemán durante la segunda guerra mundial:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Aparentemente este mensaje no tiene nada de malo y parece sin importancia pero cuando tomamos las segundas letras de esta información podemos obtener el siguiente mensaje:

Pershing sails from NY June 1

Aquí vemos lo fácil que es esconder información en textos, así como comprendemos la necesidad de gran cantidad de información (ruido) para ocultar la auténtica información de forma que no llame la atención.
Todas estas técnicas se han ido perfeccionando con el pasar del tiempo y con el aparecimiento de la información ya que este artefacto es capaz de resolver muchos caracteres en fracciones de segundos

Tinta invisible

Aunque el método de escritura con tinta invisible **es** usado desde la edad media, es en la Segunda Guerra Mundial cuando adquiere una importancia capital. Fue usado muy activamente por la resistencia en los campos de prisioneros nazis.

Generalmente se usa de la siguiente forma: en primer lugar **se escribe una carta** completamente normal, y después se escribe, entre las líneas de esa carta, otro texto donde está la información importante. Era habitual el uso de **vinagre**, **zumos de frutas** u **orina**, aunque hoy en día existen compuestos químicos específicos que sirven igualmente y no desprenden olores tan fuertes (que serían fácilmente detectados por un perro entrenado). Al **calentar** el papel, la escritura oculta se hace visible.

Micropuntos

La tecnología de los micropuntos fue inventada por los alemanes **durante la Segunda Guerra Mundial** y fue usada de forma muy activa durante la época de la **guerra fría**.

La técnica se basa en **esconder puntos minúsculos** en fotografías, tan pequeños que para el ojo humano e incluso para instrumentos ópticos básicos como lupas- resultan invisibles, pero que forman un patrón de información significativa.

Debido a la naturaleza analógica de esta técnica, resultaba fácilmente detectable para los servicios de inteligencia, si bien advertir la presencia de mensajes esteganografiados no siempre significa que puedan ser legibles. Aún así, descubrir la presencia de un mensaje esteganografiado se considera un fracaso de la esteganografía que lo soporta, pues la imposibilidad de comprender su contenido conforma su capa de cifrado.

3.3.2. Factibilidad Operacional

Actualmente la esteganografía está irremisiblemente **ligada a los ordenadores**, que le han proporcionado el medio necesario para ser efectiva, y del que durante siglos no pudo disponer. Así mismo, está **íntimamente ligada a la criptología** en general y a la criptografía en particular.

Hoy en día se usan multitud de técnicas esteganográficas, pero todas se basan en los mismos principios de ocultación de información. Este punto, al ser el eje central del documento, lo veremos en detalle más adelante.

Ahora me gustaría dejar una opinión personal sobre criptografía, esteganografía y la sociedad actual:

Como ya se comentó en el documento de *Criptosistemas Informáticos*, a los gobiernos nunca les hizo demasiada gracia la criptografía, esteganografía... y en general cualquier método que pueda suponer datos fuera de su control. Gracias a los ordenadores personales, y al software libre en gran medida, técnicas antes reservadas a unos pocos están ahora al alcance de cualquiera... hasta de las peores personas.

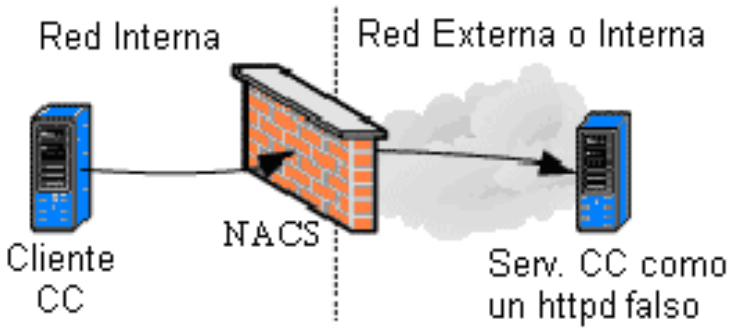
Todo esto viene por la campaña de acoso y derribo que ciertos sectores norteamericanos emprendieron contra la criptografía y esteganografía en general, especialmente contra PGP y su creador Philip Zimmermann, al publicarse que esta clase de técnicas fueron supuestamente utilizadas por la organización terrorista AlQaeda para transmitir información previa a los atentados del 11 de Septiembre en Nueva York.

Señores: no hay medios culpables, sino personas culpables. No culpen a PGP de un atentado, no menos que a Samuel Colt por inventar el revólver (eso sin entrar a analizar los usos positivos de PGP frente a los

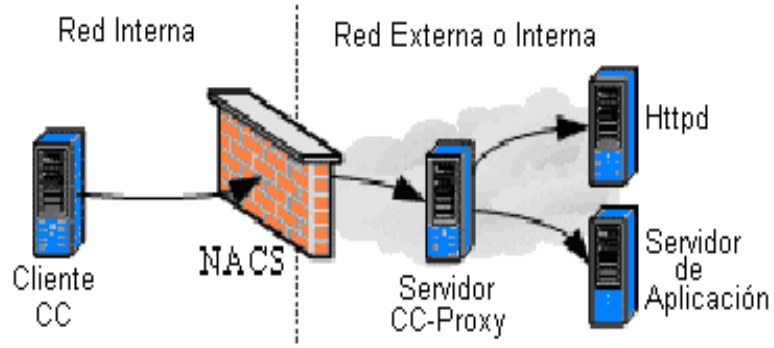
dudosos usos positivos del revólver...) o a Albert Einstein por contribuir al desarrollo de la bomba de fisión.

3.4. Desarrollo de Técnicas a nivel de Redes

A nivel de servidores las técnicas han sido aplicadas en todos los servicios que puede tener un servidor es así que podemos encontrar principalmente en los DMZ y en los servicios de las páginas WEB.



La información que pueda ser descifrada a través de un sniffer o de cualquier software de descriptación de contraseñas tiene la obligatoriedad de poder pasar un servidor firewall el cual no permite técnicas de esteganografía ya que estos tienen ENCRIPTADAS con algoritmos propios de estas funciones.



En el ejemplo anterior se puede observar una distribución completa de DMZ con todos los servidores y como antesala un firewall el mismo que precautela las contraseñas que le siguen a los servidores de proxy que es el primer servidor y el que se encarga de proteger y de brindar el recurso del internet a todos los usuarios dentro de la red.

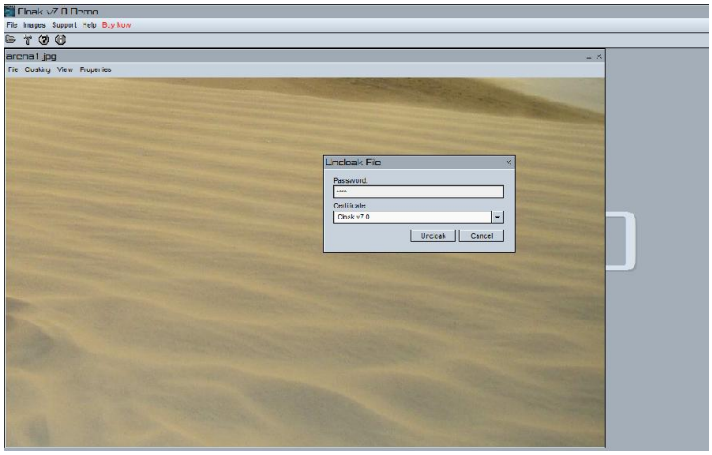
Actualmente muy pocos elementos de red tienen la posibilidad de detectar, que a los niveles superiores del modelo OSI se pueda estar pasando alguna información extraña

Son muchos los caminos por los cuales un administrador de red puede sufrir las consecuencias de un incidente de seguridad informática.

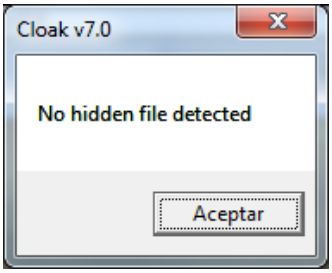
3.5. Encriptación de imágenes

En el manejo de imágenes, sonidos en nuestra investigación no ha sido tomado en cuenta ya que esto tiene que ver con las reproducciones mismas que son importantes para personas o empresas que se dedican a este tipo de actividades ya que resulta en ocasiones tan imperceptibles al ojo humano que se necesita de

ciertas cualidades que en algunas personas son innatas, en cuanto al sonido siempre se ha escuchado que existen grabaciones con mensajes diabólicos particularmente en grupos o artistas que son jóvenes y que tienen mucha llegada en los jóvenes. Pero todo este tratamiento según las paginas que se pudieron investigar es principalmente cuando en los discos de acetato que existían hace no mucho tiempo atrás se le forzaba a que girara en sentido contrario distorsionaba el sonido y por ende la vocalización de los autores y cantantes de las canciones. Para nada esto ha sido 100% comprobado pero tampoco ha sido aclarado por lo que siempre queda o se da un margen a la duda de que es lo que se hizo y que es lo que se va hacer.



En las imágenes arriba indicadas es como un sistema que se encuentra en el internet de nombre cloak hace un tester de texto dentro de la imagen para ver si puede encontrar información encubierta, ya que de esta manera se podría despejar dudas de que existe o no información camuflada dentro de un dibujo o un gráfico.



Como resultado se pudo obtener en el test de la imagen un resultado negativo ya que no se pudo encontrar ningún carácter dentro de la imagen que se trato de escanear.

3.6. Bases de la esteganografía

El desarrollo de la informática e Internet ha supuesto el marco perfecto para que la esteganografía alcance su mayoría de edad. Los avances en computación nos proporcionan medios para calcular rápidamente los cambios necesarios en la ocultación de un mensaje, e Internet proporciona los medios necesarios para transportar grandes cantidades de información a cualquier punto del planeta.

La esteganografía actual se basa en **esconder datos binarios** en la maraña de bits que supone un fichero.

Los bits que componen el mensaje a ocultar se introducen (bien sea **añadiéndolos**, o **realizando operaciones aritméticas** con los originales) en el fichero ya existente, procurando que el fichero resultante después de realizar los cambios parezca el original.

¿Cómo logramos que el fichero resultante no parezca haber sido modificado? Depende de qué tipo de fichero estemos modificando. Prácticamente **cualquier tipo de fichero** es bueno para ocultar datos en su interior, pero hay algunos (imágenes y sonido principalmente) que resultan ideales para este cometido, por motivos que más adelante comentaremos. Así mismo existen ciertos programas especializados en ocultación de información en sectores de disco no usados.

Sea cual sea el tipo de información que queramos esteganografiar, y sea cual sea el medio en el que queremos hacerlo, hay ciertas reglas básicas:

- Toda información (texto ASCII, hexadecimal, código morse...) que queramos introducir, debe ser primero **convertida a binario**. Si bien cualquier base numérica es válida, la comodidad trabajando con binario es mucho mayor.

  Nunca hay que permitir que un supuesto atacante obtenga el **fichero original** (anterior a la modificación), pues permitiría, mediante comparación, establecer pautas de cambios en la información. Esto podría llevar en última instancia a desentrañar el mensaje oculto.

- Las cabeceras de los ficheros -salvo excepciones- **NO** deben ser modificadas.

- No transmitir la **clave** o **algoritmo** esteganográfico por un medio inseguro.

Aunque la esteganografía computacional clásica consiste en la modificación binaria del fichero que sirve de canal, existen ciertas técnicas para **casos particulares** de ficheros que también son válidas (aunque **complicadas de hacer "a mano"**, con lo cual dependemos de algún tipo de software... cosa que no queremos). Un ejemplo de estas técnicas es la adición de mensajes ocultos a los ficheros de sonido mediante **superposición de capas de sonidos** que no resultan audibles para el oído humano, pero que sí contienen información.

Así mismo, también he encontrado documentación de técnicas basadas en ocultación de mensajes en **ficheros de imagen** creados con potentes programas de tratamiento gráfico (como Gimp o Photoshop) mediante el **uso de capas transparentes** donde se alojaba la información. Al igual que en el caso anteriormente citado, **no** considero esta técnica segura en absoluto.

3.7. Esteganografía avanzada

La esteganografía es un arte complejo y con muchos matices. Sin llegar aún a la combinación de esteganografía y criptografía, es posible el uso de determinadas **técnicas avanzadas** que permiten **aumentar la eficacia** de una información oculta mediante esteganografía. Veamos alguna:

Uso de múltiples claves

Esta técnica es heredada directamente de la criptografía, pero con distinta forma de aplicación. Consiste en **usar distintas codificaciones para cada porción arbitraria** del mensaje a ocultar. Así, una frase de cinco palabras puede tener una clave de codificación para cada una de las palabras: en la primera restamos una unidad en los ceros y sumamos una unidad en los unos, en la segunda realizamos lo mismo pero invirtiendo
El orden de los bits, en la tercera realizamos el XOR de los bits...

Naturalmente la clave ha de ser conocida por el destinatario.

Esteganografía en capas

Mediante esteganografía en capas **establecemos una relación lineal entre los elementos ocultos**. Así, la codificación de la segunda palabra o letra de un mensaje depende de la primera (puede depender del último valor de la cifra, del último valor modificado, de la posición...).

Así **establecemos un orden estricto de decodificación** que impide obtener completamente el mensaje sin la primera parte, con lo cual únicamente debemos comunicar la clave para obtener esta parte y la pauta a seguir para encadenar los fragmentos.

Adición de ruido

Aunque en un mensaje esteganografiado TODO el fichero es considerado ruido, podemos **añadir ruido en el proceso de esteganografiado**. Así, además de modificar los bits necesarios para inyectar nuestro mensaje, podemos **modificar unos cuantos bits aleatorios** del mensaje de forma que aún teniendo el fichero original, un posible atacante deba conocer el sistema de codificación usado.

Uso de distintas magnitudes

Aunque **lo habitual es variar en 1 bit** el byte del mensaje original, nada nos impide **variarlo en más bits**.

Así, podemos establecer claves complejas, como por ejemplo: ocultamos una frase de cinco palabras, y al ocultar la primera de las palabras sumamos 1 bit en la codificación de la primera letra, 2 bits en la codificación de la segunda, 3 bits en la tercera... hasta que vuelva a aparecer una modificación de 1 bit, que significará el inicio de otra palabra.

Mientras trabajemos con **ficheros que usen mucha información** (imágenes de 24 bits o más por ejemplo) no se notará que variemos la escala en 1 ó 10 unidades, y nos proporciona un **tipo de clave más compleja**.

Otras técnicas

Existen muchas otras técnicas esteganográficas que permiten aumentar la complejidad y seguridad, tantas como queramos idear nosotros mismos.

Lo ideal es que cada uno idee y use su propia técnica.

3.8. Esteganografía y criptografía

Como ya comentamos al principio del presente documento, la **esteganografía hoy día está íntimamente ligada a la criptografía**. Teniendo unos

conocimientos básicos de criptografía y esteganografía podemos ocultar nuestros datos con un grado de seguridad sorprendentemente alto (*NOTA: Para los interesados en la criptografía, tengo publicado un documento sobre el tema en mi web*).

Mediante **técnicas criptográficas** como las usadas por **PGP (Pretty Good Privacy)** podemos hacer nuestros datos completamente **ilegibles**, pero un fichero cifrado con PGP tiene una estructura muy específica que lo hace **reconocible de inmediato**. En ciertos países el gobierno controla a la población hasta el extremo de controlar la información que emiten a la red (por ejemplo en China), por lo que cualquier dato cifrado sería interceptado de inmediato. Podemos **comparar la criptografía a tener alarma** en casa: nuestra seguridad aumenta muchísimo, pero todos los que vean las medidas de seguridad sabrán que tenemos cosas importantes que guardar (por norma general se cifran únicamente los contenidos muy importantes).

Mediante **técnicas esteganográficas** podemos hacer que cualquier información pase **inadvertida** (subyaciendo en información inofensiva), pero la seguridad intrínseca de la esteganografía para datos importantes no es mucha.

Mediante la combinación de estas dos técnicas estableceremos **dos capas en la seguridad** de la información: la primera capa, más externa, es la **esteganográfica**; y la segunda, interna, la **criptográfica**.

Cada una de las capas tiene un cometido en esta peculiar **simbiosis**: la capa **criptográfica** se encarga de la **seguridad de los datos** (pues aunque la esteganografía sea un medio de proteger datos, no es comparable al cifrado) mientras que la capa **esteganográfica** protege la **integridad de la capa criptográfica**.

Aunque nada nos impide realizar nuestros cifrados a mano, para usar algoritmos y claves complejas es casi imprescindible el uso de **software especializado**. Yo sin duda recomiendo cualquier **implementación de openPGP**, especialmente

GnuPG que es software libre, y cuyo código fuente puede ser revisado por cualquiera que desconfíe.

Si ciframos nuestros datos de forma que nos devuelva una **armadura ASCII**, ya tendremos todos los caracteres que componen nuestro mensaje cifrado. Es **muy recomendable** que la clave que usemos para la realización de criptografía orientada a esteganografía use el **algoritmo DH/DSS** (**Diffie-Hellman** / **Digital Standard Signature**), pues el **tamaño de salida** de datos es **mucho menor**. Con la armadura ASCII del mensaje solamente necesitamos un poco de paciencia para esteganografiar los datos.

3.9. Ataques a la esteganografía

No son muchas las investigaciones publicadas acerca de métodos de ataque a la esteganografía, aunque es de esperar que debido al auge que ha experimentado hoy en día gracias a técnicas como las **marcas de agua**, se publiquen más investigaciones sobre debilidades y formas de aprovecharlas.

Los dos métodos más usados para detectar y atacar la esteganografía son:

Ataque visual

Consiste básicamente en buscar de forma manual diferencias entre el fichero original y el esteganografiado, siempre y cuando dispongamos del fichero original. En caso de no disponer de él, se pueden buscar **irregularidades** en el fichero esteganografiado para tratar de encontrar signos de la existencia de datos ocultos, pero difícilmente podremos obtener información útil más allá de la existencia de los mismos.

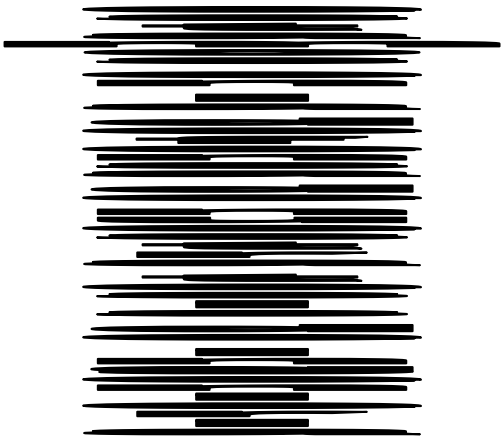
Esta técnica es la más rudimentaria a la hora de realizar análisis esteganográfico y **no tiene mucha utilidad** real.

Ataque estadístico

Este tipo de ataque se basa en el mismo concepto que el **criptoanálisis diferencial** del que hablé en *Criptosistemas Informáticos*.

El concepto de este tipo de ataques se basa en la **comparación de la frecuencia de distribución de colores** de un **fichero potencialmente esteganografiado** con la frecuencia que podríamos esperar en teoría de un fichero esteganografiado. Aunque los resultados son bastante buenos (ha demostrado en muchas ocasiones ser **efectiva**), esta técnica es **extremadamente lenta**.

Si la creación de mensajes esteganografiados a mano ya es complicada, el ataque estadístico lo es mucho más, por lo que se automatiza mediante diversos programas. Pero a nuestro favor tenemos que los programas especializados en detección y ruptura de mensajes esteganografiados suelen **buscar pautas** de mensajes ocultos con algún tipo de **software especializado** en la creación de los mismos. Si esteganografiamos nuestros mensajes a mano, la posibilidad de que la información sea recuperada ilícitamente es ínfima.
Dentro de la presente investigación se pudo obtener algunos ejemplos que en algo aclaran el verdadero significado de lo que es la esteganografia y cuál es su modo de operación.
Ejercicio 1:



Esta es una forma grafica de dar a conocer un texto en forma vertical que aparentemente es una señal de sonido, o puede ser un grafico que no tiene sentido pero si se decide rebajar el tamaño de la fuente se puede observar verdaderamente el significado de la cuenta de la esteganografía.

El texto es claro y ya legible para los ojos de los usuarios de las técnicas "Estamos en la defensa de nuestra de tesis de ingeniería".

.

E	S	E	D	T	I	G	I
S	E	F	E	R	S	E	A
T	N	E	N	A	D	N	2
A	L	N	U	T	E	I	0
M	A	S	E	E	I	E	1
O	D	A	S	S	N	R	0

Esta es otra forma de demostrar cómo trabaja la esteganografía mediante matrices las cuales son de fácil lectura si podemos leer en forma vertical el texto y resulta que nos dice: "ESTAMOS EN LA DEFENSA DE NUESTRA TESIS DE INGENIERIA 2010".

S	W	E	W	T	R	E	Q
P	I	W	W	Y	U	U	D
O	V	S	S	A	S	W	X
Y	W	B	T	A	Y	T	R
T	E	H	O	E	J	K	I
R	E	L	Ñ	K	M	J	J
A	Q	W	E	R	U	A	J
W	S	F	G	I	O	J	S

No podría faltar en este análisis de las técnicas un organigrama que desde siempre ha sido una de las técnicas de desarrollo mental.

Otras de las técnicas esteganográficas tienen que ver con ocultar texto e imágenes o archivos de música. Podríamos utilizar texto para ocultar texto también:

“Arrebato de su anillo hirió dos infantes atolondrados. Arroz y pescado aseguran apetitoso omelet”.

Si extraemos la segunda letra de cada palabra se obtendría el siguiente mensaje: “reunió tres pm”, este tipo de ejemplo fueron los que se utilizaron para los ataques del 11 de septiembre en New York a las Torres Gemelas y al Pentágono en Washington D.C.
Todos estos ejercicios de técnicas de esteganografía se utilizan como texto aparentemente inofensivo y poco importante, para evitar un mensaje que, en un determinado contexto, podría definir una estrategia bélica futura.

Sin embargo en informaciones mostradas en los grandes periódicos del mundo se pudo observar cómo se manifestaba en esta investigación en la parte superior que estas técnicas son muy utilizadas pero que siempre han sido muy bien cuidadas de parte de las autoridades y de los departamentos de defensa de los países que han sido víctimas de atentados terroristas como los Estados Unidos de América, el Reino Unido y la misma España.


USA TODAY

Home
News
Money
Sports
Life
Tech
Main Categories
Tech briefs
Web Guide
Tech Investor
Product reviews

CyberSpeak

• E-mail this story • Subscribe to the newspaper • Sign-up for e-mail news

12/19/2001 - Updated 09:30 AM ET

Bin Laden's messages could be hiding in plain sight

Now we have to worry about steganography. That's right: steganography. No not the ancient art of writing on a stegosaurus. It's a way to conceal a codes

Uso extendido

ETA no es la única organización terrorista que acude a programas de encriptación para proteger sus documentos y bases de datos.

Al Qaeda tiene incluso una aplicación propia y de distribución libre, el conocido como **Mujahidin's Secret**, capaz de codificar y enviar de forma segura todo tipo de archivos a través de internet.

También se ha detectado el uso de la esteganografía, una técnica muy antigua pero que ahora aprovecha las nuevas tecnologías y que permite camuflar información relevante en documentos, como fotografías, textos o incluso canciones, en apariencia inofensivos.

Como se puede observar esta ciencia ha suscitado mucho interés en los últimos años debido a que ha sido utilizada por organizaciones criminales y terroristas. No obstante, no se trata de ningún nuevo ingenio, se lleva empleando desde la más remota antigüedad. Este artículo pretende introducir al lector en el campo de la esteganografía, clarificando sus diferencias con la criptografía y mostrando ejemplos de software para hacer uso de esta técnica.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La esteganografía es una técnica en constante evolución, con una larga historia y con capacidad para adaptarse a nuevas tecnologías. A medida que las herramientas de esteganografía se hacen más avanzadas, las técnicas y las herramientas empleadas en el estegoanálisis también se hacen más complejas.

2. Actualmente muy pocos elementos de red tienen la posibilidad de detectar, que a los niveles superiores del modelo OSI se pueda estar pasando alguna información extraña

3. Son muchos los caminos por los cuales un administrador de red puede sufrir las consecuencias de un incidente de seguridad informática.

4. Se demostró cómo el protocolo http, puede pasar información oculta e incluso distribuir dicha información a varias personas que se encuentren distantes sin ser detectadas.

5. No existe solo una sino muchas formas de realizar canales ocultos en protocolos de niveles altos.

6. La Esteganografía ha aparecido ante los ojos de mucha gente, a raíz de los hechos del 11 de septiembre y la posibilidad de que redes terroristas estén usando algunas de estas técnicas para transmitir mensajes a través de imágenes y sonidos en la red, hacen que el uso legal o ilegal de la Esteganografía sea un tema debatido en grupos de seguridad

7. En la Universidad Técnica de Cotopaxi y en la Carrera de Ingeniería en Informática y Sistemas Computacionales son muy pocos los temas de este tipo que se desarrollan ya que no existe la suficiente bibliografía para poder sustentar temas de esta naturaleza eminentemente prácticos.

8. Dentro de la presente investigación hemos podido darnos cuenta que la esteganografia es una técnica muy importante pero que todavía falta de desarrollar ya que no es muy fácil descifrar y no se puede encontrar software adecuado para que haga esta actividad o que permita a ciencia cierta demostrar el mensaje o cuadro de imagen que era la que se buscaba.

9. Los ejemplos que aquí se presentan son muy fáciles de hacerlos pero resultan muy difíciles de aplicarlos y de traducirlos para los usuarios finales.

10. En lo que va de la tecnología se encuentran muchos algoritmos de encriptación y de descencriptación pero en ninguno de los casos, estos son aplicados a la realidad de la Universidad o de la provincia en general como se demuestra en la entrevista desarrollada a los señores docentes de la Carrera.

RECOMENDACIONES

1. Para la adquisición de políticas de esteganografía se debe tomar muy en cuenta los equipos con que cuentan las instituciones o las empresas ya que las capas del modelo OSI tiene mucho que ver en cómo se asignan contraseñas a nivel de hardware para luego hacerlo a nivel de software.

2. Los atentados que han venido sufriendo las grandes potencias económicas a nivel mundial se basaron en técnicas parecidas a la cual hemos estudiado, pero en el internet todavía se pudo observar la falta de aplicaciones que puedan facilitar la visualización de esta información camuflada en gráficos, sonidos, o en el mismo texto que son enviado en correos electrónicos de forma inofensiva pero que llevan un transfundo.

3. Las páginas WEB que tienen un formato de hipertexto es decir las http siempre han tenido la peculiaridad de ser inseguras ya que han sido abiertas con algunos software que se pueden bajar sin costo alguno desde el internet y esto ha conllevado a aplicar las más diversas técnicas de ocultamiento y de encriptación de contraseñas o de manipulación de la información de forma general.

4. No existen en nuestro país bibliografía que permita abrir el horizonte en técnicas que puedan ayudar a solventar el ocultamiento de la información o la manera más optima de generar contraseñas que permitan prevenir los ataques que se han vuelto muy comunes como se pudo observar en la investigación que se realizo.

5. LA Universidad Técnica de Cotopaxi a través de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas debería fomentar el tratamiento de nuevos temas de investigación ya que estos pueden ser una buena base de bibliografía en la biblioteca de la institución lo que ayudaría a las nuevas generaciones de ingenieros en Informática.

6. La esteganografía es una técnica muy útil al momento de generar contraseñas seguras pero su y tratamiento resulta ser muy complicado ya que no permite seguir un estándar único para el desarrollo de aplicaciones que vayan en beneficio de las personas que desean explorar un poco más.

GLOSARIO

Abort

Fracaso, interrupción, cancelación, aborto

Acceso Físico

Es el medio utilizado para obtener información de las oficinas, salas de cómputo, escritorios y archivos.

Acceso Lógico

Es el medio utilizado para obtener información de las bases de datos y sistemas de información de la organización.

Activos

Son los recursos de la organización. Existen varios tipos de activos como son: Los recursos de información (bases de datos, los documentos de sistemas), los recursos de software (software de sistemas operativos, herramientas de desarrollo), activos físicos (equipamiento informático, equipos de comunicaciones, otros) y servicios (iluminación, energía eléctrica, etc.)

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

ASIC

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.

Asignaciones de amplitud de banda

La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Anomalía

Irregularidad en el funcionamiento de un sistema, de un software, de un control, etc.

Camino Forzado

Ruta limitada entre una Terminal de usuario y los servicios del computador. Evita que los usuarios seleccionen rutas fuera de la trazada entre su Terminal y los servicios a los cuales esta autorizado a acceder.

Canal Oculto

Es un cauce de comunicación que permite a un proceso receptor y a un emisor intercambiar información de forma que viole la política de seguridad del sistema;

esencialmente se trata de un método de comunicación que no es parte del diseño original del sistema pero que puede utilizarse para transferir información a un proceso o usuario que a priori no estaría autorizado a acceder a dicha información.

Clave Pública

Clave que puede ser revelada a cualquier persona.

Clave Secreta

Clave que debe mantenerse en secreto.

Código Troyano

Es un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado.

Comercio Electrónico

Consiste en la compra, venta, marketing y suministro de información complementaria para productos o servicios a través de redes informáticas.

Computación Móvil

Se define como la serie de artefactos y equipos portátiles, hardware, que hacen uso de la computación para lograr su funcionamiento, así, se tiene a las computadoras portátiles, los teléfonos celulares, los cuadernos de notas computarizados, las calculadoras de bolsillo, etc.

Criptografía

Dícese de la ciencia que estudia la forma de codificar y descodificar documentos, de forma que sólo puedan ser leídos por la persona que posee la clave de descodificación.

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.
Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

Data datos

Data Mining minería de datos

Database base de datos, banco de datos

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Esteganografía

Del griego "steganos" (secreto) y "grafía" (escrito). También llamada cifra Encubierta. Es el arte y ciencia de escribir mensajes secretos de tal forma que nadie fuera de quien lo envía y quien lo recibe sabe de su existencia, en contraste con la criptografía, en donde la existencia del mensaje es clara pero está obscurecido. Por lo general un mensaje de este tipo parece ser otra cosa, como una lista de compras, un artículo, una foto, etc.

Evaluación de Riesgos

Es un proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse, obteniendo la información necesaria para que el empresario esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y, en tal caso, sobre el tipo de medidas que deben adoptarse. La evaluación de riesgos consta de una fase llamada de análisis de riesgos (identificación de peligros y estimación de los riesgos) y una fase posterior de valoración de riesgos y de control de riesgos si fuese posible.

Evidencia

Datos, registros, declaraciones de hecho o cualquier otra información que respaldan la existencia o veracidad de algo.

LDAP

("Lightweight Directory Acces Protocol", en español Protocolo Ligero de Acceso a Directorios)

Es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

Se usó inicialmente como un Front-end o interfaz final para x.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

Incidente

Dícese del fallo que sucede en un equipo o sistema de manera temporal o aleatoria, sin que existan unos motivos claros para ello.

Procesamiento de Información

Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida.
Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados.

Seguridad Informática

Conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionales. Estos daños incluyen el acceso a bases de datos de personas no autorizadas, el mal funcionamiento del hardware y la perdida física de datos.

Seguridad de la Información

La seguridad de la información consiste en proteger uno de los principales activos de cualquier empresa: la información. La seguridad de la información es requisito previo para la existencia a largo plazo de cualquier negocio o entidad. La información es usada en cada uno de los ámbitos empresariales, los cuales dependen de su almacenamiento, procesado y presentación.

Servicio de Información

Un servicio para los sistemas que proporciona un sistema de base de datos para los archivos de configuración comunes.

Servicio de Red

Es un servicio para que cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes.

Sistema de Información

ci

Conjunto de elementos, ordenadamente relacionados entre sí que aporta al sistema objeto, es decir, a la organización a la cual sirve y le marca directrices de funcionamiento, la información necesaria para el cumplimiento de sus fines, para lo cual tendrá que recoger, procesar y almacenar la información, facilitando la recuperación de la misma.

Sistema Informático

Es aquel sistema que se encarga del manejo de información en la computadora, a través de la cual el usuario controla las operaciones que realiza el procesador.

Sistema Operativo

Termino que se utiliza para referirse al conjunto de programas interrelacionados, que se dedican a controlar las funciones básicas del sistema, las operaciones de bajo nivel y el manejo de archivos sin necesidad de que intervenga un operador.

Software Malicioso

Software que ha sido deliberadamente diseñado para producir un resultado defectuoso o dañoso para el usuario. Incluye tanto la categoría genérica de los virus informáticos, como la del llamado spyware.

Trabajo Remoto

Se refiere al trabajo que una persona realiza por fuera de su puesto de trabajo normal.

Utilitarios del Sistema

Reconstruir índices, compactar y validar bases de datos, validar consistencia de datos, cambiar fecha de operación y del sistema, importar y exportar datos entre empresas, transferir productos, precios, existencias de almacén y acceso al generador de reportes.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:

Ethernet 10 Mbps

Fast Ethernet 100 Mbps

Gigabit Ethernet 1000 Mbps

4.4.- BIBLIOGRAFÍA

- Orígenes de la esteganografía, Maria Jesus Villagran, VS Antivirus

  http://www.vsantivirus.com/esteganografia

  Tomado el: 06 Nov. 2008.

- Esteganografía

  http://geneura.ugr.es/~jmerelo/atalaya/esteganografia.htm

  Tomado el: 06 Nov. 2008.

- Trabajo Practico ”Estaganografia”, Universidad John F. Kennedy, Argentina, 1998

4.4.1. - WEB BIBLIOGRAFÍA

- http://badc0ded.org.ar/steg/
- http://www.monografias.com/steganografia.html
- www.lordepsylon.net
- h ttp://www.death-master.tk/
- http://www.gnu.org/copyleft/fdl.html
- http://www.death-master.tk
- http://www.gnu.org/copyleft/fdl.html
- http://www.sfreedom.net/~hpn/foro/index.php?act=ST&f=6&t=746