



La revista de la comunidad de programación en español



Como instalar la replica de la base de datos en MySql

Creación de archivos de ayuda HTML compilados



Creando un servidor remoto mediante Visual Basic .NET

Conectar flashremoting a postgresql con php



Saber que versión del .NET Framework estamos utilizando

Boletín de software libre

manuales, códigos, noticias, elaces...

**Seguridad Informatica
Capítulo II. CRIPTOLOGÍA**

Prohibida su venta
Totalmente libre



1 5 0 5 2 0 0 6



0 0 0 7

EDITORIAL

Octava edición digital de **MYGNET-MAGAZINE Junio 2006**

Presentamos una vez más la publicación digital correspondiente a este mes, esperamos que sea de su agrado, hemos incluido una sección de manuales donde se listan todos los que fueron publicados en el mes y a demás nos complace presentar el capítulo II de seguridad informática, "Criptología".

Mandamos nuestros cordiales saludos y agradecimientos a todos los colaboradores que han participado con nosotros, de igual manera para todas las personas que nos han echo llegar sus comentarios que nos han sido de mucha utilidad, a nombre del equipo de mygnet les damos las gracias...

Reiteramos nuevamente la invitación para que participen con nosotros.

Editores

Martín Roberto Mondragón Sotelo.

martin@mygnet.com

Gustavo Santiago Lázaro.

gustavo@mygnet.com

Escribenos a *info@mygnet.com*

Visítanos a *<http://www.mygnet.com>* o *<http://www.mygnet.org>*

CONTENIDO

Aplicaciones

Como instalar la replica de la base de datos en MySql	3
Creación de archivos de ayuda HTML compilados	5
Crear un Server Remoto con NET	9

Programación

FlashRemoting y postgres	11
Saber que versión del .NET Framework estamos utilizando	14
Códigos fuentes en el mes	15

Seguridad

Seguridad informática. Capítulo 2. Criptología.....	24
---	----

Boletín

Boletín Software libre	39
Noticias del mes.....	42
Manuales del mes.....	51
Enlaces del mes.....	60

Como instalar la replica de la base de datos en MySql

Autor: Fredy Ramirez Porfirio
 Perfil del colaborador
 Nombre: Fredy Ramirez Porfirio
 País: MÉXICO 
hosh.frp@gmail.com

Personalidad: Serio, sincero y bastante social. | **Nivel de estudios:** Licenciatura o profesional | **Área de estudio:** Ing. en Sistemas Computacionales | **Experto en:** C/C++ , VC++, VB, Java, ActionScript | **Conocimientos:** Flash, Flash Communication Server, ensamblador, bash, postgresql, MySQL, MatLab y tratamiento de imágenes | **Pasatiempo(s):** Leer y navegar por internet.

Este tutorial en particular describe cómo instalar la réplica de la base de datos en MySQL. La réplica de MySQL permite tener una copia exacta de una base de datos de un servidor principal (maestro) en otro servidor (esclavo), y todas las actualizaciones a la base de datos en el servidor principal se repliegan inmediatamente a la base de datos en el servidor auxiliar de modo que ambas bases de datos estén sincronizadas. Esto no es una política de respaldo porque si se corre un comando de borrado de forma accidental también será realizado en el esclavo; sin embargo las réplicas pueden ayudar a proteger contra faltas de hardware. En este tutorial en particular se mostrara como replegar la base de datos alumnos contenida en una PC con la dirección IP 192.168.0.16 a un esclavo. Ambos sistemas (maestro y esclavo) están funcionando en Windows XP SP2.

Ambos sistemas tienen MySQL 5.0 instalado, y la base de datos alumnos con las tablas y los datos ya existente en el maestro, pero no en el esclavo. Primero quisiera decir que ésta no es la única manera de levantar la configuración de tal sistema. Hay muchas maneras de alcanzar esta meta pero ésta es la manera que utilizaremos.

Configurar el Maestro:

Primero tenemos que corregir "C:\Archivos de programa\MySQL\MySQL Server 5.0\my.ini". Tenemos que permitir el establecimiento de una red para MySQL, y MySQL debe escuchar en todas las direcciones IP, por lo tanto comentamos estas líneas (si es que existen):

```
#skip-networking
#bind-address = 127.0.0.1
```

Además tenemos que decirle a MySQL de qué base de datos debe escribir a los registros (estos registros son utilizados por el esclavo para ver qué ha cambiado en el maestro), que fichero de diario debe utilizar, y tenemos que especificar donde esta el servidor maestro de MySQL. Deseamos replegar la base de datos alumnos, así que ponemos las líneas siguientes en "C:\Archivos de programa\MySQL\MySQL Server 5.0\my.ini":

```
log-bin = C:\Archivos de programa\MySQL\MySQL Server 5.0\mysql-bin.log
binlog-do-db=alumnos
server-id=1
```

Después de haber echo esto, detenemos el servidor y posteriormente lo volvemos a cargar, para que este aplique los cambios recién establecidos.

Después entramos en la base de datos de MySQL como root y creamos el usuario con privilegios de la réplica:

```
mysql -u root -p
Enter password:
```

Ahora estamos en el shell de MySQL.



```
GRANT REPLICATION SLAVE ON *.* TO 'slave_user'@'%' IDENTIFIED BY '<password>';
FLUSH PRIVILEGES;
Reemplace <password> con el password real.
```

Después haga esto (aún en shell de MySQL):

```
USE alumnos;
FLUSH TABLES WITH READ LOCK;
SHOW MASTER STATUS;
```

El comando pasado mostrará algo como esto:

```
+-----+-----+-----+-----+
| File      | Position | Binlog_do_db | Binlog_ignore_db |
+-----+-----+-----+-----+
+ mysql-bin.006 | 183      | alumnos      |                    |
+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

¡Anote esta información, la necesitaremos más adelante en el esclavo!

Salimos del shell de MySQL:

```
quit;
```

Pasando la información existente en del maestro al esclavo.

Hay dos formas para pasar las tablas y los datos existentes de alumnos en el maestro al esclavo. El Primer debe hacer una descarga de la base de datos, El segundo debe utilizar el comando `LOAD DATA FROM MASTER;` en el esclavo. El último tiene la desventaja de que la base de datos en el maestro será bloqueada durante esta operación, así que si se tiene una base de datos grande en un sistema de producción de mucho trafico, esto no es lo que se desea, y en este caso recomiendo seguir el primer método. Sin embargo, el último método es muy rápido, así que aquí describiré ambos.

Primer método:

```
mysqldump -u root -p<password> --opt alumnos > alumnos.sql
```

Reemplace <password> con el password real para el usuario root de MySQL

Importante: No hay espacio entre -p y <password>!

Esto creará una descarga del SQL del alumnos en el archivo alumnos.sql, para que ¡Transfiera este archivo a su servidor esclavo!. Si desea usar esta manera `LOAD DATA FROM MASTER;` entonces por ahora no hay nada que se deba hacer.Finalmente tenemos que abrir las tablas en alumnos.

Configurando el esclavo.

En el esclavo primero tenemos que crear la base de datos alumnos:

```
mysql -u root -p
Enter password:
CREATE DATABASE alumnos;
quit;
```

Si ha hecho una descarga del SQL de alumnos en el maestro para transferirla al esclavo, entonces es hora de importar la descarga del SQL en nuestra base de datos alumnos creada en el esclavo:

```
mysql -u root -p<password> alumnos < /path/alumnos.sql
```

Reemplace <password> con el password real para el usuario root de MySQL

Importante: No hay espacio entre -p y <password>!

Path se refiere a la dirección donde se encuentra el archivo con la descarga del SQL.

Ahora tenemos que decirle a MySQL en el esclavo que sea el esclavo, que el maestro es 192.168.0.16, y que la base de datos principal a mirar es alumnos. Por lo tanto agregamos las líneas siguientes a "C:\Archivos de programa\MySQL\MySQL Server 5.0\my.ini":

```
server-id=2
master-host=192.168.0.16
master-user=<slave_user>
master-password=<user_password>
master-connect-retry=183
replicate-do-db=alumnos
```

Reiniciamos MySQL.



Si no ha importado alumnos de la base de datos maestra con la ayuda de una descarga del SQL, tal vez desee usar esta manera `LOAD DATA FROM MASTER;` entonces es hora de conseguir los

datos de la base de datos maestra, así que entramos en el shell MySQL del esclavo:

```
mysql -u root -p
Enter password:
LOAD DATA FROM MASTER;
quit;
```

Si tiene phpMyAdmin instalado en el esclavo puede comprobar si todas las tablas de datos de la base de datos alumnos del maestro están también disponible en la base de datos alumnos del esclavo.

Finalmente, debemos hacer esto:

```
mysql -u root -p
Enter password:
SLAVE STOP;
```

En el comando siguiente (aún en el shell de MySQL) tiene que sustituir los valores apropiadamente:

```
CHANGE MASTER TO MASTER_HOST='192.168.0.16',
MASTER_USER='slave_user', MASTER_PASSWORD='<password>',
MASTER_LOG_FILE='mysql-bin.006', MASTER_LOG_POS=183;
```

MASTER_HOST es la dirección IP o el nombre de la máquina del maestro (en este ejemplo es 192.168.0.16).

MASTER_USER es el usuario al que le concedimos derechos de réplica en el maestro.

MASTER_PASSWORD es la contraseña de MASTER_USER en el maestro.

MASTER_LOG_FILE es el archivo MySQL que se devuelve al ejecutar `SHOW MASTER STATUS;` en el maestro.

MASTER_LOG_POS es la posición MySQL que se devuelve al ejecutar `SHOW MASTER STATUS;` en el maestro.

Ahora todo que se tiene que hacer es inicializar el esclavo. Todavía en el shell de MySQL funcionando:

```
START SLAVE;
quit;
```

Ahora siempre que la base de datos alumnos sea actualizada en el maestro, todos los cambios serán replagados a la base de datos alumnos en el esclavo.

Por ahora esto es todo, espero que les sirva.

Saludos...

Creación de archivos de ayuda HTML compilados



Filiberto Ugarte Castañeda
fugartex@hotmail.com
País: MÉXICO

Nivel de estudios: Licenciatura o profesional | **Área de estudio:** Lic. en Electrónica | **Objetivo(s):** Aprender cada día mas y obtener los mejores beneficios para quienes estén involucrados(as). | **Experiencia laboral:** Sistemas, bases de datos, páginas web, archivos compilados HTML de ayuda. | **Experto en:** Siempre hay algo que aprender. | **Actividades:** Capacitación continua autodidacta en lenguajes de computación, sistemas y equipos, traducción de aplicaciones. | **Conocimientos:** C, Pascal, Ensamblador para microcontrolador 8051/8052, HTML, CSS, VRML, Just BASIC v1.01, JavaScript, Visual Basic 6.0, Programación en escalera de PLCs, Windows, Ubuntu Linux 5.10, Mandriva Linux 10.1, Puppy Linux 1.0.1 | **Idioma(s):** Inglés 80%, Esperanto (principiante) | **Pasatiempo(s):** Convivencia con mi esposa y mi hijo, Star Wars, cine, música.

El desarrollo actual de aplicaciones profesionales requiere que sean acompañadas por sistemas de ayuda que permitan facilidad y claridad de uso por parte del usuario, logrando una curva de aprendizaje eficaz.

Los archivos de ayuda HTML compilados, con extensión chm y sucesores de aquellos con extensión hlp, contribuyen a construir estos sistemas de ayuda, con los que se puede integrar multimedia y todas las prestaciones que se pueden obtener al usar archivos HTML.

Para producir esta clase de archivos usaremos la aplicación Microsoft HTML Help Workshop que está disponible en forma gratuita en el siguiente vínculo:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=00535334-c8a6-452f-9aa0-d597d16580cc&DisplayLang=en>

El archivo de instalación es htmlhelp.exe. Una vez descargado el archivo y realizada su instalación, se crearán accesos directos a dos aplicaciones: "HTML Help Workshop" y "HTML Help Image Editor". Esta última es una aplicación para realizar captura y procesamiento básicos de imágenes, como fue el caso de las capturas de pantalla para este artículo.

Abre la aplicación HTML Help Workshop y elige File > New en el menú principal. En el cuadro de diálogo selecciona "Project" para iniciar el asistente para nuevos proyectos.

En el primer paso deja sin elegir "Convert WinHelp Project" ya que deseamos construir un proyecto desde cero. Esta opción solo se marca si vas a convertir un archivo de ayuda en formato HLP a este formato CHM.



En el segundo paso, se elige la dirección y el nombre del proyecto. Crea una carpeta para contener todos los archivos del proyecto, elige esa carpeta y escribe como nombre del proyecto Ayuda.hhp



En el tercer paso, se indican los archivos de tabla de contenido (.hhc), de índice (.hhk) y html (.htm) para agregarlos al proyecto. Como aún no existen, deja sin seleccionar estas tres opciones.



En el cuarto paso se llega a la finalización del asistente.



Al terminar el asistente, aparecerá una pantalla donde se resumen las características del proyecto en forma de tres pestañas "Project", "Contents" e "Index". En la pestaña Project en la sección [OPTIONS] se observa que el archivo de ayuda se llamará Ayuda.chm.



Tabla de Contenido

Para crear la tabla de contenido (los temas y páginas) de nuestro proyecto, oprime la pestaña Contents.



Es aquí donde se especifica qué archivo se usará como tabla de contenido. Como en este proyecto todavía no existe, elige la opción "Create a new contents file",

llama a este archivo "Ayuda.hhc" y guárdalo en la misma carpeta del proyecto.

Índice

Para crear el índice (la búsqueda de temas) de nuestro proyecto, oprime la pestaña Index.



Es aquí donde se especifica qué archivo se usará como índice. Como en este proyecto todavía no existe, elige la opción "Create a new index file", llama a este archivo "Ayuda.hhk"

y guárdalo en la misma carpeta del proyecto.

De regreso a la pestaña Project, notarás que ya fueron agregados los archivos Ayuda.hhc y Ayuda.hhk. Guarda todo tu proyecto oprimiendo en el menú principal File > Save Project.

Agregado de Entradas en Tabla de Contenido

Para empezar a construir nuestro archivo de ayuda vamos a escribir un archivo htm para que sea desplegado en el archivo Ayuda.chm. En el menú principal, elige File > New y selecciona HTML File en el cuadro de diálogo. Se crea un archivo htm básico y en un cuadro de diálogo se te pide el título de este archivo htm. Escribe "Introducción" como título

y acepta este cambio. Entre las etiquetas <BODY> y </BODY> escribe "Introducción". El archivo htm quedará como sigue:

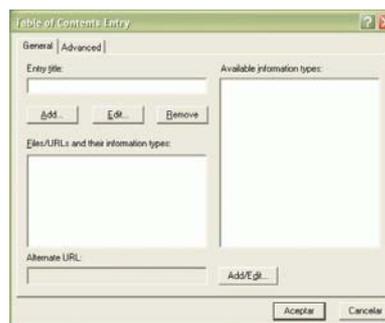
```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
<HTML>
<HEAD>
<meta name="GENERATOR" content="Microsoft®; HTML Help Workshop 4.1">
<Title>Introducción</Title>
</HEAD>
<BODY>

Introducción

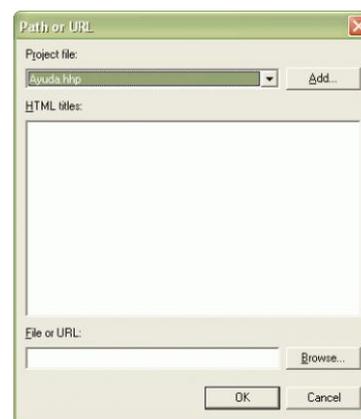
</BODY>
</HTML>
```

Guarda este archivo htm (File > Save File) en la misma carpeta de tu proyecto con el nombre Introduccion.htm. Cierra este archivo.

Ahora oprime la pestaña Contents y elije el tercer botón desde arriba hacia abajo con la imagen de una hoja de papel con interrogación y que indica "Insert a page" en su texto para abrir la ventana "Table of Contents Entry".



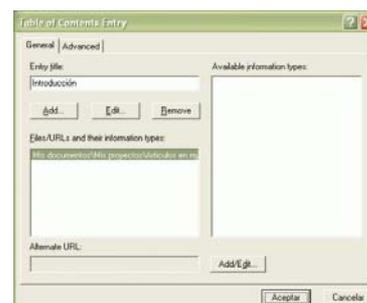
En el cuadro de texto "Entry title" escribe Introducción. Cada entrada en la tabla de contenido está asociada con un archivo htm. Esta entrada, Introducción, tendrá asociado el archivo Introduccion.htm. Para hacer esto, oprime el botón Add... y se desplegará la ventana "Path or URL".



En esta ventana oprimiendo el botón Browse, busca y selecciona el archivo Introduccion.htm. Acepta esta asignación y tendrás una ventana como esta:

Acepta los cambios y verás que la entrada Introducción ya fue integrada a tu proyecto. Este archivo Introduccion.htm, además, tiene que ser agregado al proyecto. Para esto, en la pestaña Project, selecciona el segundo botón desde arriba hacia abajo que indica "Add/Remove topic files" y en la ventana "Topic Files" oprime el botón Add... para seleccionar el archivo Introduccion.htm. Después de aceptar los cambios, verás una nueva sección llamada [FILES] donde se lista el archivo Introduccion.htm.

Compilación inicial



Antes de guardar y compilar por primera vez tu proyecto, oprime la pestaña Project y selecciona el primer botón de arriba hacia abajo que indica "Change Project Options" para abrir la ventana "Options".

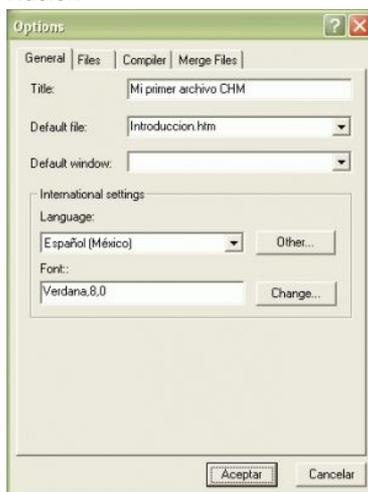
En la pestaña "General" de la ventana "Options" escribe los siguientes datos:

Para tener título del archivo de Ayuda.chm, en el cuadro de texto Title escribe "Mi primer archivo CHM".

El primer archivo que se desplegará al abrir el archivo de ayuda es Introduccion.htm. Esto indícalo en la lista desplegable Default file.

Selecciona la fuente y su tamaño con los que se desplegará la tabla de contenido oprimiendo el botón Change.

Realiza los cambios necesarios para el idioma de acuerdo a tu Nación.



Guarda ahora el proyecto completo y selecciona File > Compile. En la ventana "Create a compiled file" de ser necesario oprime el botón Browse... para indicar la carpeta y el nombre del archivo Ayuda.hhp



Oprime el botón Compile. Si no existen errores, se despliega el informe de la compilación y se creará el archivo Ayuda.chm que podrás abrir al explorar la carpeta de tu proyecto.

Vamos a aumentar nuestro proyecto

agregando un tema (heading) con su respectiva página. Crea dos nuevos archivos htm con las siguientes características, guárdalos en la misma carpeta donde estamos trabajando y agrégalos a tu proyecto.

Nombre de archivo	Título	Texto en cuerpo (BODY)
Tema1.htm	Tema 1	Tema 1
Tema1Pagina1.htm	Tema 1 – Página 1	Página 1 de Tema 1

Ahora en la pestaña Contents selecciona la entrada Introducción y oprime el segundo botón de arriba hacia abajo con el icono de carpeta y cuyo texto es "Insert a heading". Responde No a la pregunta "Do you want to insert this entry at the beginning of the table of contents?" ya que deseamos que se coloque a continuación de la entrada Introducción y se abrirá la ventana "Table of Contents Entry" vista anteriormente. Escribe Tema 1 en el cuadro "Entry title" y

asóciate el archivo Tema1.htm. Selecciona ahora el botón "Insert a page" y en la ventana "Table of Contents Entry" escribe "Página 1" en el cuadro "Entry title" y asóciate el archivo Tema1Pagina1.htm.

De este modo puedes seguir agregando los temas y las páginas que tu archivo de ayuda necesite y haciendo uso de los botones con las flechas "Move selection up" y "Move selection down" (para organizar el orden de los temas y sus páginas); y "Move selection right" y "Move selection left" (para organizar la jerarquía de los temas y sus páginas con respecto a los demás).



Personalización de Tabla de Contenido

Es posible hacer distinguir cada entrada con una imagen diferente para denotar a primera vista su contenido. Vamos a hacer que el icono de la entrada Introducción tenga una hoja de papel con la letra i para señalar que contiene información inicial. Selecciona esta entrada y elige el cuarto botón de arriba

hacia abajo con la imagen de un lápiz y cuyo texto indica "Delete selection" para desplegar la ventana "Table of Contents Entry" y a continuación oprime la pestaña "Advanced". Explora las opciones del control Image index para ver todas las imágenes que se pueden desplegar y selecciona la imagen 17. Haz lo mismo para la entrada "Página 1" cambiando su imagen con la 11. Cabe hacer notar que en esta misma ventana puedes convertir una página en encabezado y viceversa con la opción "Change entry to a heading" o "Change entry to a page" según sea el caso.

Para cambiar el comportamiento y la apariencia general de la tabla de contenido oprime el primer botón de arriba hacia abajo cuyo texto indica "Contents properties" para desplegar la ventana "Table of Contents Properties". Veremos las pestañas "General" y "Styles".

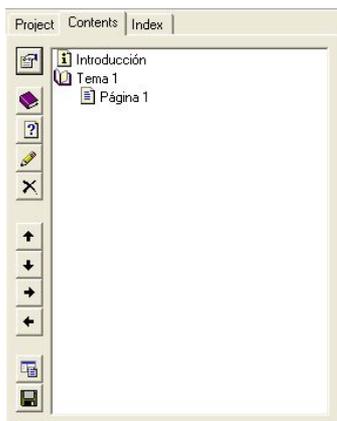
Para la pestaña "General", quita la marca en la opción "Use folders instead of books" para desplegar la imagen de los temas como libros en lugar de carpetas. Aquí también puedes elegir una imagen personalizada para los temas y seleccionar el estilo y tamaño de fuente para ellos.



Para la pestaña "Styles", en el listado "Window Styles" se encuentran los comportamientos visuales que hasta el momento tiene tu tabla de contenido. Aquí puedes agregar otros como "Only expand a single heading" con lo que al expandir un tema, los demás se contraen; o "Draw lines between items" que hará que se dibujen líneas de jerarquía, como un árbol, entre los temas y sus páginas. También puedes elegir los colores de primer y segundo plano. Realiza los cambios que desees y acepta los cambios en la ventana.



La ventana de tu proyecto se verá como esta:



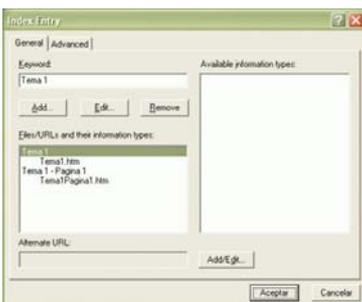
Guarda y compila tu proyecto para ver los cambios.

Agregado de Entradas en el Índice

Para alimentar las entradas del índice, se procede de manera similar al proceso de tabla de contenido. Oprime la pestaña "Index" y oprime el segundo botón de arriba hacia abajo con la imagen de una llave y cuyo texto

indica "Insert a keyword" para desplegar la ventana "Index Entry".

En el cuadro de texto "Keyword" escribe "Tema 1" y seguidamente oprime el botón Add... para elegir el o los archivos htm donde se mencione la palabra Tema 1. Para este caso habrá dos archivos que tienen esa referencia: Tema1.htm y Tema1Pagina1.htm.

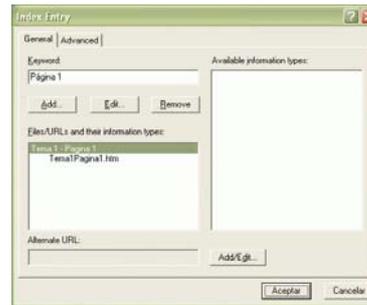


Agrega ahora otra entrada al índice con la palabra clave "Pagina 1". Al hacerlo se te preguntará si deseas agregar esta entrada al inicio del índice (Do you want to insert this entry at the beginning of the index?). Responderemos

que Si y en esta nueva entrada la palabra clave será Página 1 asociándola con el archivo Tema1Pagina1.htm.

Guarda el proyecto y compílalo para ver los cambios. Al oprimir en el Índice en la palabra clave "Pagina 1" se desplegará el archivo asociado, mientras que al oprimir en la palabra "Tema 1" se mostrará una ventana donde se puede elegir entre dos ubicaciones dentro del archivo de ayuda porque a esta palabra clave le referenciamos precisamente dos archivos htm.

De este modo se le asignan al índice todas las palabras claves que sean convenientes, ordenándolas y jerárquizándolas para



incluirlos en tus proyectos y de este modo crear archivos de ayuda mas profesionales con mayores recursos y palabras claves.

De la misma forma que para la tabla de contenido, con el primer botón de arriba hacia abajo con el texto "Index properties" se

puede especificar la fuente y su tamaño con los que se desplegarán los temas del índice.

Notas

Es muy conveniente utilizar editores mas poderosos para HTML, sean WYSIWYG o no, para crear los archivos html necesarios con sus imágenes, sonidos, cursores, hojas de estilo en cascada, guiones JavaScript o VBScript, etc.

La descompilación (en caso de que exista esta palabra), File > Decompile, de los archivos chm con esta aplicación extrae todos los archivos del proyecto, el archivo .hnc de tabla de contenido y el archivo .hhk, pero no el archivo de proyecto .hnp, por lo que es muy importante que respaldes todos tus archivos para poder actualizar tus archivos de ayuda.

Para finalizar, éste es el código que se incorpora en Visual Basic al procedimiento del evento Click de un control de menú llamado Ayuda, para desplegar tu archivo de ayuda:

```
Private Sub Ayuda_Click()
```

```
    Dim strRutaArchivo As String
    ' Variable de cadena para designar
    ' la dirección del archivo de ayuda
```

```
    strRutaArchivo = "C:\Ayuda.chm"
```

```
    Shell "hh.exe " & strRutaArchivo, vbMaximizedFocus
```

```
End Sub
```

Podrás hallar los archivos Ayuda.chm, Ayuda.hnc, Ayuda.hhk, Ayuda.hnp, Introduccion.htm, Tema1.htm, Tema1Pagina1.htm y el artículo en formato pdf en

<http://www.mygnet.com/codigos/editoresweb/22>

Ojala que este artículo te sea útil. Saludos.

Etapas

Primero pensé que un maestro debía tener razón en todo.

Despues percibí que mi maestro estaba equivocado en muchas cosas.

Después me di cuenta de lo negativo y de lo positivo.

Lo negativo era permanecer en cualquiera de las dos primeras etapas.

Lo positivo era transmitir esto a todos.

Crear un Server Remoto con NET

Autor: David Ordinola
davidordinola@yahoo.es
País: PERÚ 

Nivel de estudios: Posgrado | Área de estudio: Ingeniería Informática | Experto en: .Net | Actividades: Desarrollador | Idioma(s): Español, Inglés | Reconocimiento(s): MCAD

Creando un servidor remoto mediante Visual Basic .NET

En este artículo se muestra cómo crear un servidor remoto sencillo al que puede tener acceso otra aplicación. La aplicación que tiene acceso a este servidor puede estar en el mismo equipo, en otro equipo o en otra red. El servidor remoto se divide en dos partes: el objeto de servidor y la aplicación de servidor. El objeto de servidor es el objeto con el que se comunica el cliente y la aplicación de servidor se utiliza para registrar el objeto de servidor con el motor de tiempo de ejecución Remoting.

Requisitos

En la lista siguiente se describe el hardware, el software, la infraestructura de red y los ServicePack recomendados que se necesitarán:

Visual Studio .NET

En el presente artículo se da por supuesto que está familiarizado con los temas siguientes:

Visual Studio .NET

Visual Basic .NET

Redes

Crear un objeto de servidor remoto

El primer paso para crear la aplicación de servidor consiste en crear el objeto de servidor. El objeto de servidor es la instancia que crea la aplicación cliente y con el que se comunica en el equipo servidor. La aplicación cliente lleva esto a cabo a través de un objeto proxy que se crea en el cliente. En este ejemplo, el objeto de servidor reside en una Biblioteca de clases (DLL) y se llama myRemoteClass.

1. Cree una nueva aplicación de biblioteca de clases en Visual Basic .NET. Se creará Class1 de forma predeterminada.
2. En el Explorador de soluciones, cambie el nombre del archivo de código Class1.vb a ServerClass.vb.
3. Abra ServerClass.vb y cambie el nombre Class1 a myRemoteClass. myRemoteClass debe heredarse de la clase MarshalByRefObject. Esta clase debe aparecer del siguiente modo:

```
Public Class myRemoteClass
Inherits MarshalByRefObject
End Class
```

4. Agregue un método público a myRemoteClass, que toma una cadena, muestra un mensaje en la consola con un valor de la cadena y devuelve True si la

cadena no está vacía.

```
Public Class myRemoteClass
Inherits MarshalByRefObject
Public Function SetString(sTemp As String) As Boolean
Try
Console.WriteLine("Esta cadena '{0}' tiene una longitud de {1}",
sTemp, Len(sTemp))
Return (sTemp <> "")
Catch
Return (False)
End Try
End Function
End Class
```

5. Genere el proyecto para crear el ensamblado ServerClass.dll.

6. Guarde y cierre el proyecto.

Crear una aplicación de servidor remoto

Después de crear el objeto de servidor con el que se comunicará el cliente, debe registrar este objeto con el marco de trabajo Remoting. Al registrar el objeto, también debe iniciar el servidor y hacer que el servidor escuche en un puerto a los clientes que intentan conectarse a ese puerto.

Para ello, necesita un tipo de proyecto que cree un archivo ejecutable. El objeto de servidor se incluye en un proyecto independiente, de manera que pueda crear fácilmente una referencia al objeto de servidor desde el proyecto del cliente. Si incluye el objeto de servidor en este proyecto, no puede hacer referencia a él, ya que las referencias sólo se pueden establecer en archivos DLL.

Para simplificar, cree una nueva aplicación de consola en Visual Basic .NET para iniciar el servidor remoto. Se creará Module1 de forma predeterminada.

En el Explorador de soluciones, cambie el nombre del archivo

```
Module1.vb a ServerObject.vb.
```

Agregue una referencia al espacio de nombres

```
System.Runtime.Remoting.
```

Agregue una referencia al ensamblado ServerClass.dll que creó en la sección anterior.

Utilice la instrucción Imports de los espacios de nombres Remoting, Remoting.Channels y Remoting.Channels.Tcp de forma que no tenga que suministrar declaraciones de dichos espacios de nombres más adelante en el código. Debe utilizar la instrucción Imports antes que cualquier otra declaración.

```
Imports System.Runtime.Remoting
Imports System.Runtime.Remoting.Channels
Imports System.Runtime.Remoting.Channels.Tcp
```

Declare la variable apropiada. Para ello, declare e inicialice un objeto TcpChannel que escuche si los clientes se conectan a un puerto determinado, que en este ejemplo es el puerto 8085.

Utilice el método RegisterChannel para registrar el canal con los servicios de canal. Agregue el siguiente código de declaración al procedimiento Main del módulo predeterminado:

```
Dim chan As TcpChannel = New TcpChannel(8085)
ChannelServices.RegisterChannel(chan)
```

Llame al método RegisterWellKnownType del objeto RemotingConfiguration para registrar el objeto ServerClass con el marco de trabajo Remoting y especifique los parámetros siguientes en el código:

a. El nombre de tipo completo del objeto que se va a registrar (que es ServerClass.myRemoteClass en este ejemplo), seguido del nombre de ensamblado ServerClass. Especifique tanto el nombre del espacio de nombres como el nombre de la clase. Como no especificó un espacio de nombres en la sección anterior, se utilizará el espacio de nombres raíz predeterminado.

b. Asigne al extremo donde se va a publicar el objeto el nombre RemoteTest . Los clientes necesitan conocer este nombre para conectarse al objeto.

c. Utilice el modo de objeto SingleCall para especificar el parámetro final. El modo de objeto especifica la duración del objeto cuando se activa en el servidor. En el caso de los objetos SingleCall, se crea una nueva instancia de la clase para cada llamada realizada por un cliente, aunque el mismo cliente llame al mismo método más de una vez. Por el contrario, los objetos Singleton se crean sólo una vez y todos los clientes se comunican con el mismo objeto.

```
RemotingConfiguration.RegisterWellKnownServiceType( _
Type.GetType("ServerClass.myRemoteClass, ServerClass"), _
"RemoteTest", _
WellKnownObjectMode.SingleCall)
```

Utilice el método ReadLine del objeto Console para que la aplicación de servidor siga en ejecución.

```
Console.WriteLine("Presione <ENTRAR> para salir...")
Console.ReadLine()
```

Genere el proyecto.

Guarde y cierre el proyecto.

FlashRemoting y postgres



Roberto Torres Sanchez
iuka@hotmail.com
País: MÉXICO

Nivel de estudios: Licenciatura o profesional

Flash Remoting y Postgres

Utilizaremos flashremoting para hacer una conexión con una base de datos que esta contenida en postgresSQL utilizando algunas clases de nuestros amigos de mygnet.

Bueno una vez que esta configurado flash remoting (véase en el articulo flash Remoting y AMFPHP escrito por Gustavo santiago) y postgresSQL continuaremos.
Crearemos una base datos en postgresSQL con las tablas de usuarios, equipos, recursos, catalogo, prestamos.

Creamos un archivo php Y ponemos este código, para crear el puente hacia nuestros servicios que iremos creando(utilizando un pequeño sistema de inventario):

```
<?php
class mygnet_component
{
function mygnet_component()
{
    $this->methodTable = array( "login" => array( "description" => "login",
        "access"=> "remote", "arguments" => array ("usuario","clave")
    ), "usuarios" => array( "description" => "usuarios", "access"=> "remote",
    "arguments" => array () ),
    "equipos" => array( "description" => "equipos", "access"=> "remote",
    "arguments" => array () ),
    "recursos" => array( "description" => "recursos", "access"=> "remote",
    "arguments" => array () ),
    "catalogo" => array( "description" => "catalogo", "access"=> "remote",
    "arguments" => array () ),
    "prestamos" => array( "description" => "prestamos", "access"=> "remote",
    "arguments" => array () ),
    );
}

$conexion =pg_connect("user= password= dbname=")or die("no puedo
conectarme con la bese de datos");
} //fin del arreglo de componentes

function login($usuario,$clave)
{
$resultado=pg_query("SELECT * FROM usuarios WHERE
usu_login='".$usuario.'" AND usu_pass='".$clave.'"") or die("error");
if($row=pg_fetch_array($resultado)){return 1; }else{return 0; }
}

function usuarios()
{
$resultado=pg_query("SELECT * FROM usuarios") or die("error");
while($row=pg_fetch_array($resultado))
{ $persona[]=array( "id"=>$row["usu_id"],
                    "name"=>$row["usu_nombre"],
                    "apellido"=>$row["usu_apellidos"],
                    "login"=>$row["usu_login"],
                    "Password"=>$row["usu_pass"],
                    "fecha"=>$row["usu_fecha"]
                    );
}
}
```

```

return $persona;
}

function equipos()
{
$resultado=pg_query("SELECT * FROM equipo") or die("error");
$i=0;
while($row=pg_fetch_array($resultado))
    { $equipo[]=array( "id"=>$row["equip_id"],
"descripcion"=>$row["equip_descripcion"],
                    "numserie"=>$row["equip_serie"],
                    "codebar"=>$row["equip_codebar"],
                    "fecha"=>$row["equip_fecha"]
                    );
    }
return $equipo;
}

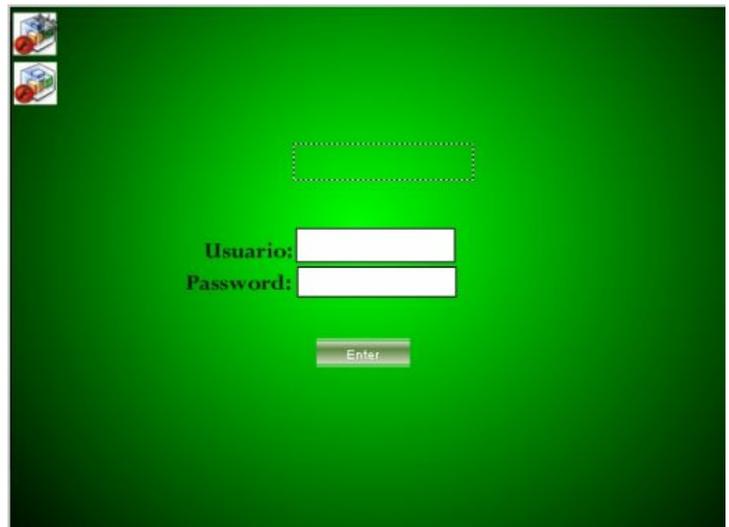
function recursos()
{
$resultado=pg_query("SELECT * FROM recursos") or die("error");
$i=0;
while($row=pg_fetch_array($resultado))
    { $recurso[]=array("id"=>$row["rec_id"],
"descripcion"=>$row["rec_descripcion"],
"cantidad"=>$row["rec_cantidad"],
"fecha"=>$row["rec_fecha"]
    );
    }
return $recurso;
}

function catalogo()
{
$resultado=pg_query("SELECT * FROM catalogo") or die("error");
$i=0;
while($row=pg_fetch_array($resultado))
    { $cata[]=array("id"=>$row["cequip_id"],
"equipo"=>$row["cequip_equipo"]
    );
    }
return $cata;
}

function prestamos()
{
$resultado=pg_query("SELECT
usu_nombre,equip_descripcion,prest_salida,prest_entrega,prest_id,prest_entrega FROM prestamo,usuarios,equipo WHERE
prestamo.usu_id=usuarios.usu_id AND
prestamo.equip_id=equipo.equip_id") or die("error");
$i=0;
while($row=pg_fetch_array($resultado))
    { $prestamo[]=array("id"=>$row["prest_id"],
"usuario"=>$row["usu_nombre"],
"equipo"=>$row["equip_descripcion"],
"salida"=>$row["prest_salida"],
"entrega"=>$row["prest_entrega"]
    );
    }
return $prestamo;
}
}
}
?>

```

A continuación desarrollaremos la interfaz en flash8



Una vez creada agregaremos las clases de flashremoting (remotingclasses y remotingdebugclasses) encima del fotograma y al mismo tiempo agregaremos el siguiente código sobre las acciones del fotograma (parte de AS2)

```

import mx.remoting.NetServices;
import mx.remoting.Connection;
mx.remoting.debug.NetDebug.initialize();
NetServices.setDefaultGatewayUrl("http://localhost/flashservices/gateway.php");

conn = NetServices.createGatewayConnection();
serv = conn.getService("mygnet_component",this);
_global.bandera=0

function login_Result(result)
{
if(result==0){msg="Datos incorrectos"}
else {
    _global.bandera=1;
    gotoAndPlay(2)
}
}

_global.limpiar=function()
{
    _root.cargador.myDataGrid.removeAllColumns();
    _root.cargador.myDataGrid.removeAll();
}

_global.usuarios=function() { serv.usuarios();
}

function usuarios_Result(result)
{
for(i=0; i<result.length; i++)
    {
    _root.cargador.myDataGrid.addItem({Id:result[i]['id'],Nombre:result[i]['name'],
Apellido:result[i]['apellido'],login:result[i]['login'],Password:result[i]['Password'],
Fecha:result[i]['fecha']});}
}
_global.equipo=function() { serv.equipo();
}

```

```

}

function equipos_Result(result)
{
for(i=0; i<result.length; i++)
{
_root.cargador.myDataGrid.addItem({Id:result[i]['id'],Nombre:resu
lt[i]['descripcion'],Numserie:result[i]['numserie'],Codigo de barra:res
ult[i]['codebar'],Fecha:result[i]['fecha']});
}
}

_global.recursos=function() { serv.recursos();
}

function recursos_Result(result)
{
for(i=0; i<result.length; i++)
{
_root.cargador.myDataGrid.addItem({Id:result[i]['id'],Nombre:resu
lt[i]['descripcion'],Cantidad:result[i]['cantidad'],Fecha:result[i]['fec
ha']});
}
}
_global.catalogo=function() { serv.catalogo();
}

function catalogo_Result(result)
{
for(i=0; i<result.length; i++)
{
_root.cargador.myDataGrid.addItem({Id:result[i]['id'],Nombre:resu
lt[i]['equipo']});
}
}

_global.prestamos=function() { serv.prestamos();
}

function prestamos_Result(result)
{
for(i=0; i<result.length; i++)
{
_root.cargador.myDataGrid.addItem({Id:result[i]['id'],usuario:resu
lt[i]['usuario'],equipo:result[i]['equipo'],salida:result[i]['salida'],entr
ega:result[i]['entrega']});
}
}

stop();

```

Y para verificar el usuario y su contraseña pones en el botón el siguiente código.

```

on(press)
{
serv.login(usu,contra);
}

```

Agregamos una nueva capa y en el fotograma2 crearemos un cargador para mandar a llamar la película de menú con el sig. Código

```

if(_global.bandera==0)gotoAndPlay(1);
onEnterFrame()
{
loadMovie("menu.swf","cargador");
}

stop();

```

Y por ultimo crearemos el menú utilizando un datagrid y combobox



Insertando el código en sus acciones del fotograma:

```

myDataGrid.dataProvider = recordSetInstance;
tablas = new Object();

tablas.change = function (evt)
{
switch(evt.target.selectedIndex)
{
case 0: _global.limpiar();_global.usuarios();break;
case 1: _global.limpiar();_global.equipos();break;
case 2: _global.limpiar();_global.recursos();break;
case 3: _global.limpiar();_global.catalogo();break;
case 4: _global.limpiar();_global.prestamos();break;
}
}
menu.addEventListener("change", tablas);

```

Descarga el ejemplo completo

<http://www.mygnet.com/codigos/actionscript/18/>

Saber que versión del .NET Framework estamos utilizando



Juan Francisco Berrocal
berrocal239@hotmail.com
País: REPÚBLICA DOMINICANA 🇩🇲

Personalidad: Un tipo que le gusta su trabajo y con una visión clara de la vida | **Nivel de estudios:** Técnico superior universitario | **Área de estudio:** Tec. En Programación y Operación de Microcomputadoras | **Objetivo(s):** Seguir aprendiendo cada día mas de mi pasión mas grande LA PROGRAMACION | **Meta(s):** Deseo realizar un proyecto donde converjan varias plataformas, y por que no, crear mi propio lenguaje de programación | **Experiencia laboral:** Soporte IT/Software | **Experto en:** VB, VB.NET | **Actividades:** Bueno la unica actividad que realizo es programar muchas Windows Application en lenguajes .NET (es mi pasión) | **Conocimientos:** C/C++, HTML, VBScript, SQL, VB, VB.NET, C#.NET, VF | **Idioma(s):** Ingles 70%

En primer lugar saludos a toda la comunidad de desarrolladores de .NET y los que no son de .NET también, en este artículo (el cual es muy sencillo) pretendo mostrar un uso muy importante que nos brinda la clase Environment, esta nos permite revisar que versión del framework tenemos instalado en nuestro equipo.

En caso que sea desde una WindowsApplication

Sin mas preámbulos nos dirigimos a lo que nos interesa el código, este lo podemos hacer desde un Button.

Código en VB.NET

```
Private Sub btnVer_Click(ByVal sender As System.Object, _
    ByVal e As System.EventArgs) Handles btnVer.Click

    'Mostramos la información en un MessageBox
    MessageBox.Show("La Versión del Framework:" & " " &
        Environment.Version.ToString, "Saber Versión del Framework")

End Sub
```

La información en pantalla se mostrara de la siguiente manera

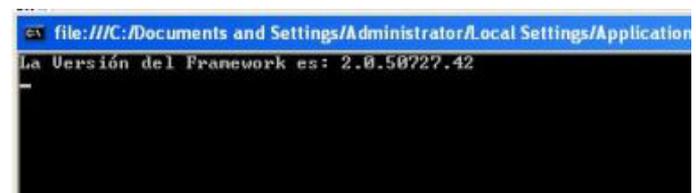


En caso de que la quieras mostrar en una ConsoleApplication

El Código es el siguiente

```
Sub Main()
    'Accedemos mediante el Metodo "WriteLine"
    System.Console.WriteLine("La Versión del Framework es:" & " " &
        Environment.Version.ToString())
    'Usamo el Metodo "ReadLine" para leer la cadena que envia
    "WriteLine"
    System.Console.ReadLine()
End Sub
```

La Aplicación corriendo se vería así.



El porque de esto: Con la salida de VS.NET la programación Windows dio un giro de 360 grados en cuanto a Performance, Código manejado, Diseño y Estructura y algo muy importante Distribución, así es, a la hora de distribuir nuestro ejecutable debemos verificar que este corra bajo el mismo Framework en el que fue trabajado, además esto lo podemos agregar como una característica utilitaria a las aplicación Cliente/Servidor que realicemos.

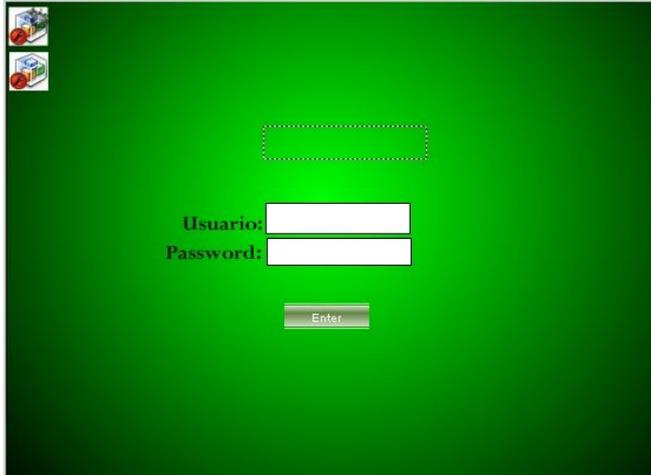
Códigos fuentes en el mes

Lenguaje Actionscript

Conexiones remotas

Flashremoting

Roberto Torres Sanchez
iuka@hotmail.com



Tamaño: 435 KB

Conexión a una base de datos postgresql con php
<http://www.mygnet.com/pages/down.php?cod=1646>

Lenguaje Asp.net

Documentos xml

Mete Tus Imágenes En Ficheros Xml .net 'bininxml'

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 105 KB

Mete tus imágenes en un fichero xml como si se tratara de un fichero de recursos, si el tamaño no es un problema, es una buena opción.

<http://www.mygnet.com/pages/down.php?cod=1644>

Cadena De Conexión En Xml Vs .ini Con (xpath)

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 11 KB

Antiguamente muchos de nosotros guardábamos la cadena de conexión en un fichero .ini y por que no hacerlo en un fichero xml.

<http://www.mygnet.com/pages/down.php?cod=1643>

Trabajando Con Xml Dom (manipulación De Xml)

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 4 KB

En este ejemplo se nos muestra como manipular un xmldocument, en el podemos ver la interacción de elementos borrado y modificación de los mismos y mas cosas.

<http://www.mygnet.com/pages/down.php?cod=1642>

.net

Creando Thumbnails De Imágenes En Asp.net

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 2 KB

Ejemplo de thumbnails escrito en vb.net: thumbnails consiste en la previsualización de imágenes de menor tamaño de las originales, esta técnica se utiliza frecuentemente para mostrar galerías de imágenes.

<http://www.mygnet.com/pages/down.php?cod=1641>

Progressbar Personalizado De Asp.net

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 14 KB

Un control personalizado de tipo progressbar para asp.net, el cual, nos muestra opcionalmente el porcentaje.

<http://www.mygnet.com/pages/down.php?cod=1640>

Mostrando Una Hoja Excel En Un Datagrid

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 17 KB

Este ejemplo muestra como mostrar una hoja excel en un datagrid por medio de una conexión oledb.

<http://www.mygnet.com/pages/down.php?cod=1639>

Visor Y Gestor De Imágenes En Asp .net

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 116 KB

Visualiza una lista de imágenes, a las cuales, se les puede modificar una serie de parámetros, comentarios, tamaño etc.

<http://www.mygnet.com/pages/down.php?cod=1638>

Maestro Detalle Con Xml*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 19 KB

Sencillo ejemplo de cómo implementar un maestro detalle en asp.net, los datos son cargados de ficheros xml para poder ver el ejemplo sin necesidad de una base de datos.

<http://www.mygnet.com/pages/down.php?cod=1637>

Añadir Un Textbox En Ejecución Asp.net*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 9 KB

Este pequeño ejemplo nos muestra, cómo añadir una caja de texto en tiempo de ejecución a un webform.

<http://www.mygnet.com/pages/down.php?cod=1636>

Propiedades Del Navegador*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 2 KB

Este ejemplo en asp.net nos muestra la lista de todas las propiedades del navegador actual, y la descripción de las mismas (tipo de navegador, versión, s.o, si acepta java script...) entre otras.

<http://www.mygnet.com/pages/down.php?cod=1635>

Multiple File Upload*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 2 KB

Este ejemplo nos muestra, como realizar un upload de varios ficheros simultáneos al servidor.

<http://www.mygnet.com/pages/down.php?cod=1634>

Explorador De Directorios En Asp.net*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 2 KB

Un buen ejemplo en que se nos muestra un simple pero eficaz explorador de ficheros y directorios realizado en asp.net.

<http://www.mygnet.com/pages/down.php?cod=1633>

Cómo Mostrar Un Datagrid De Asp.net En Excel*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 12 KB

Este ejemplo nos muestra como exportar un datagrid realizado en asp.net a excel mediante la función response.write.

<http://www.mygnet.com/pages/down.php?cod=1632>

Firma Digital Xml*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 26 KB

Este ejemplo realizado con visual web developer 2005 express edition nos muestra como implementar una firma y chequeo de la misma mediante las herramientas de .net framework 2.0.

<http://www.mygnet.com/pages/down.php?cod=1631>

Llamada De Datos De Orígenes Xml Hacia Dos Datagrid (uno Dentro De Otro)*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 14 KB

Interesante ejemplo en el que se nos muestra como realizar una llamada de datos hacia dos datagrid (uno dentro de otro) desde orígenes de datos xml.

<http://www.mygnet.com/pages/down.php?cod=1630>

Upload File (subiendo Archivos)*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 3 KB

En este pequeño ejemplo se nos muestra lo sencillo que es realizar el upload de un fichero en visual studio 2005, mostrándonos también las propiedades del archivo subido.

<http://www.mygnet.com/pages/down.php?cod=1629>

Subiendo &visualizando Imágenes Hacia/desde La Base De Datos.*Cesar Gutierrez**cesar.leandro@gmail.com*

Tamaño: 230 KB

En el siguiente ejemplo se nos muestra como insertar imágenes (previamente descargadas) directamente en la base de datos, y la visualización de las mismas mediante un gridview.

<http://www.mygnet.com/pages/down.php?cod=1628>

Lenguaje C

Linux

Comunicacion Paralelo*Daniel Enrique Velazquez Borja**dvelazquez@linuxmail.org*

Tamaño: 2 KB

Es el mismo programa que el publicado para comunicacion asincrona, solo que ahora utilizando el puerto paralelo. en lugar de enviar la informacion a tx se envian 5 bits por el puerto db-25. igual se compila con: gcc archivo.c -Incurses pero necesitas primero como su: modprobe parport_pc. si automaticamente crea /dev/parport0 solo dale chmod 777 /dev/parport0 y si no lo crea automaticamente entonces: ln -s /dev/parport0 /dev/parport0

<http://www.mygnet.com/pages/down.php?cod=1668>

Comunicacion Serial Asincrona*Daniel Enrique Velazquez Borja**dvelazquez@linuxmail.org*

Tamaño: 2 KB

Programa disenhad para comunicar mi lap con un pic16f877a para control de 4 motores en un vehiculo de navegacion via ssh, muy sencillo, lo unico que hace es enviar los bytes de comando al pic. para compilarlo pues ya sabes: gcc archivo.c -Incurses. no le

he hecho cambios a la velocidad de transferencia, así que por favor comenta si tu sabes como.

<http://www.mygnet.com/pages/down.php?cod=1626>

Lenguaje C#

Formularios

Manejo De Formularios En C#

Juan Francisco Berrocal
berrocal239@hotmail.com

Tamaño: 43 KB

Aquí muestro como manejar formularios mediante código en c#.net, este código es válido para las versiones 1.0, 1.1, 2.0 del framework, pero el mismo lo desarrolle con la versión express de c# 2005, que utiliza el la beta 2 del framework 2.0

<http://www.mygnet.com/pages/down.php?cod=1621>

.net

Manejo De Excepciones De Error En C# .net 2005

Juan Francisco Berrocal
berrocal239@hotmail.com

Tamaño: 18 KB

Aquí muestro como manejar las excepciones de error desde c#

<http://www.mygnet.com/pages/down.php?cod=1678>

Lenguaje C++

Métodos de ordenación

Sudoku

Ezequiel Hernandez
ezequielher@yahoo.com

Tamaño: 753 B

El sudoku: la gracia está en no repetir el mismo número en vertical ni horizontal ni dentro de cada grupo de 3 x 3.

<http://www.mygnet.com/pages/down.php?cod=1593>

Punteros

Copiar Cadena Con Funcion Y Punteros

Evelyn Llumitasig
evelyneli86@gmail.com

Tamaño: 445 B

Realizar un programa que copie una cadena en otra. utilizar para ello una función copiad con dos parámetros que sean punteros a caracteres.*!

<http://www.mygnet.com/pages/down.php?cod=1652>

Comparacion De Cadenas Con Punteros

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 589 B

Realizar un programa que compare dos cadenas de caracteres. utilizar una función comparar las cadenas de caracteres s y t y devuelva un valor negativo, cero o positivo si s es lexicográficamente menor que, igual a, o mayor que t

<http://www.mygnet.com/pages/down.php?cod=1651>

Estructura Con Punteros

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 465 B

//estructura con punteros

<http://www.mygnet.com/pages/down.php?cod=1650>

Intercambio De Variables Con Funcion Y Punteros

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 300 B

Intercambio de variables con función y punteros

<http://www.mygnet.com/pages/down.php?cod=1649>

Punteros

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 570 B

Considerar el problema de buscar un número en una lista de enteros utilizando la búsqueda binaria. utilizar expresiones de punteros para acceder a valores individuales en vez de referirnos explícitamente a elementos individuales de la formación. visualizar la posición del vector en la que se encuentra dicho número. el proceso será repetitivo.

<http://www.mygnet.com/pages/down.php?cod=1648>

Matriz Con Punteros

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 1 KB

Matriz con punteros

<http://www.mygnet.com/pages/down.php?cod=1647>

Css

Links En Css

Emanuel
emax_093@hotmail.com

Tamaño: 1 KB

Este código te ayudara a definir el color de tus links, espero que les sirva :)

<http://www.mygnet.com/pages/down.php?cod=1669>

Lenguaje Delphi

Manejo de base datos

Ocultar Aplicacion En Delphi A Lado Del Reloj

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 1 KB

Un sencillo truco en la que se puede colocar la aplicacion a la hora de minimizarla en el reloj en vez de star en la barra de tareas
<http://www.mygnet.com/pages/down.php?cod=1602>

Buscar Datos En Una Bd Desde Delphi

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 936 B

Una sencilla busqeda
<http://www.mygnet.com/pages/down.php?cod=1601>

Modificar Datos De Una Bd(acces) Dsde Delphi

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 1 KB

Muestro una snquilla forma de insertar datos dsde delphi en una tabla en acces
<http://www.mygnet.com/pages/down.php?cod=1596>

Eliminar Datos En Delphi

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 977 B

Muestro una snquilla forma de eliminar datos dsde dlphi
<http://www.mygnet.com/pages/down.php?cod=1595>

Insertar Datos En Una Bd(acces) Desde Delphi

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 1 KB

Un sencillo codigo que nos llevara a una aplicacion final muestro como detalladamente se insertan datos dsd delphi
<http://www.mygnet.com/pages/down.php?cod=1594>

Virus y troyanos

Codigo Fuente Littlewitch

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 351 KB

Aqui les dejo el codigo fuente de uno de los mejores troyanos que e conocido espero que les sirva.
<http://www.mygnet.com/pages/down.php?cod=1659>

Editores web

Como Crear Tablas Redondas En Html

Emanuel
emax_093@hotmail.com

Tamaño: 17 KB

Aquí les dejo un codigo de como crear tablas redondas en html. muy fácil, espero que les sirva
<http://www.mygnet.com/pages/down.php?cod=1671>

Compiladores e intérpretes

Creacion De Archivos De Ayuda Html Compilados

Filiberto Ugarte Castañeda
fugartex@hotmail.com

Tamaño: 600 KB

Archivos de proyecto, tabla de contenido e indice para crear un archivo de ayuda html compilado con la herramienta microsoft html help workshop. incluye en formato pdf el artículo completo y los archivos html del ejemplo.
<http://www.mygnet.com/pages/down.php?cod=1590>

Flash communicator

20lines Chat

Javi Santos
jsantos@oxigeno.ws

Tamaño: 46 KB

Chat en flashcom en 20 lineas tutorial en pdf
<http://www.mygnet.com/pages/down.php?cod=1676>

Lenguaje Java

Ejemplo De Ajax

David Ordinola
davidordinola@yahoo.es

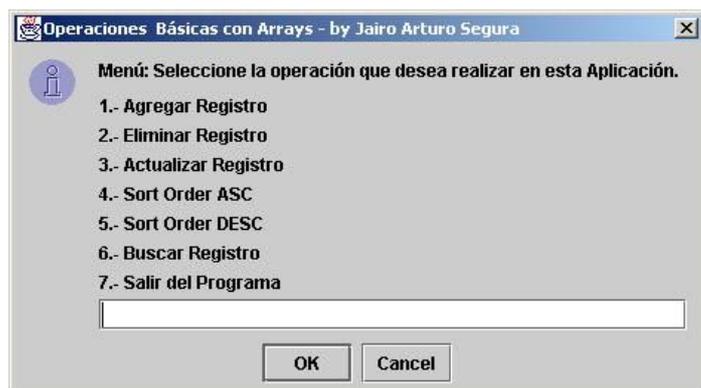
Tamaño: 1,021 KB

Un pequeño pero muy visible ejemplo de como implementar un ajax, con el codigo para que lo vean, ah el q no sabe q es ajax le recomiendo manuales/variros temas/tecnologia ajax
<http://www.mygnet.com/pages/down.php?cod=1661>

Métodos de ordenación

Menu De Opciones Usando Switch Case &Gui

Lsc Jairo Arturo Segura Morales
lscjairo.segura@gmail.com



Tamaño: 5 KB

Recuerdan los primeros menús que hacíamos en c++ con switch case??? pues aquí esta nuevamente pero ahora en java. ja gran diferencia cierto. :-p pero en fin este sistema tiene 7 funciones diferentes y maneja arreglos para almacenar los datos del programa(rustico no?). las funciones son: 1.- agregar registro (si tiene 10 elementos te avisa que el array ya esta lleno) 2.- eliminar registros (te da la opción de que selecciones la posición del registro a eliminar, si la posición seleccionada sale del rango del array te avisa, si el array esta vacío te notifica también) 3.- actualizar registro (actualiza los datos del array en la posición seleccionada por el usuario, si la posición seleccionada sale del rango del array te avisa, si el array esta vacío te notifica también) 4.- ordenar de manera ascendente con el método de la burbuja 5.- ordenar de manera descendente con el método de la burbuja 6.- búsqueda (busca un valor x en el array y te notifica cuantos elementos coinciden y en que posición se encuentra, si el array esta vacío te notifica, si no se encontraron coincidencias también te notifica) en este programa se usa: ciclo for, ciclo do while, switch case, operadores lógicos, funcion array.length para saber el tamaño de un arreglo, redimensionar arreglos, system.exit (0) para evitar que se quede colgado el programa, uso del try, uso de gui, entre otras cosas mas. espero les sea de utilidad.... ojo no cuenta con control de errores

<http://www.mygnet.com/pages/down.php?cod=1620>

Juegos

Juego Craps

Hugo

hugomora34@hotmail.com

Tamaño: 2 KB

Simulación del juego de casino craps hecho en java

<http://www.mygnet.com/pages/down.php?cod=1673>

Lenguaje Javascript

Window Alerte En Javascript

Emanuel

emax_093@hotmail.com

Tamaño: 181 KB

Aquí les dejo algo sobre los windows alerts.

<http://www.mygnet.com/pages/down.php?cod=1672>

Navegadores

Anexar A Favoritos

Lsc Jairo Arturo Segura Morales

lscjairo.segura@gmail.com

[Anexar SPROCOM a Favoritos](#)



Tamaño: 869 B

Rutina sencilla hecha en javascript la cual permite anexar un sitio web al listado favoritos.

<http://www.mygnet.com/pages/down.php?cod=1592>

Lenguaje Php

Criptografía

Cifrado De Vigenère

Martin R. Mondragón Sotelo

martin@mygnet.com

CIFRADO DE VIGENÈRE

Clave: **ESUNSECRETO**

Texto en claro: **COMUNIDAD MYGNET**

Texto cifrado: **GGGHFMFRH ACYHRL**

Tamaño: 577 B

El sistema de cifrado de vigenère (en honor al criptógrafo francés del mismo nombre) es un sistema polialfabético o de sustitución múltiple. este tipo de criptosistemas aparecieron para sustituir a los monoalfabéticos o de sustitución simple, basados en el caesar, que presentaban ciertas debilidades frente al ataque de los criptoanalistas relativas a la frecuencia de aparición de elementos del alfabeto. el principal elemento de este sistema es la llamada tabla de vigenère, una matriz de caracteres cuadrada con dimensión. la clave del sistema de cifrado de vigenère es una palabra de letras, , del alfabeto utilizado anteriormente; esta palabra es un elemento del producto cartesiano (veces), que es justamente el alfabeto del criptosistema de vigenère. de esta forma, el mensaje a cifrar en texto claro ha de descomponerse en bloques de elementos - letras - y aplicar sucesivamente la clave empleada a cada uno de estos bloques, utilizando la tabla anteriormente proporcionada.

<http://www.mygnet.com/pages/down.php?cod=1675>

Cifrado Del Kama-sutra

Martin R. Mondragón Sotelo
martin@mygnet.com

CIFRADO DE KAMASUTRA

alfabeto:

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

Texto en claro: COMUNIDAD MYGNET

Texto cifrado: MQCESGXVX CPISUZ

Tamaño: 554 B

Una de las descripciones más antiguas de encriptación por sustitución está en el kama-sutra, un texto escrito el siglo iv d.c. por el sabio hindú vatsyayana, sin embargo basado en manuscritos datados de más de 800 años (séc. iv a.c.). el kama-sutra recomienda que las mujeres estudien 64 artes, incluyendo la culinaria, la forma de vestir, masaje y la preparación de perfumes. la lista también incluye algunos artes menos obvios como prestidigitación, ajedrez, encuadernación de libros y carpintería. en la lista, la de número 45 es la mlecchita-vikalpa, el arte de la escritura secreta, indicada para ayudar las mujeres a esconder los detalles de sus relaciones. una de las técnicas recomendadas es la de formar pares aleatorios de letras del alfabeto y después sustituir cada letra del texto original por la correspondiente en el par.

<http://www.mygnet.com/pages/down.php?cod=1674>

Monitorización

Captura Direcciones Ip De Una Lan

Ismael
elclon3000@hotmail.com

Tamaño: 422 KB

Este programa sencillo en php, permite capturar todas las direcciones ip de una lan y guardarlas en una bdd q esta en mysql, existen algunas formas para hacer funcionar el programa, una de las mas faciles es intarlar el xamp (servidor web, php, mysql)

<http://www.mygnet.com/pages/down.php?cod=1589>

Lenguaje Vb

Vbskinpro V2.0

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 213 KB

Este la verdad no es un codigo sino un componente ocx, este

aunque no lo e probado deve ser muy bueno. sirve para modificar la apariencia de el form de visual basic.

<http://www.mygnet.com/pages/down.php?cod=1677>

Elite Spy

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 106 KB

De verdad que tengo suerte de haverme descargado un buen paquete de mas de 1000 codigos, lastima que pesa mas de 50 mb pero este programa es el mejor que e visto, sirve para espiar procsos y un monton de opciones mas. muy recomendable.

<http://www.mygnet.com/pages/down.php?cod=1665>

Easy Register

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 16 KB

Un pequeño programa dedicado a modificar el registro

<http://www.mygnet.com/pages/down.php?cod=1664>

App Spy

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 17 KB

Un exelente codigo fuente de un programa que espia todos los procesos y arranques del sistema.

<http://www.mygnet.com/pages/down.php?cod=1662>

Archivos y directorios

Varios

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 7 KB

Diferentes codigos para la interaccion de archivos, registro, etc

<http://www.mygnet.com/pages/down.php?cod=1654>

Exporta Listview Al Excel

William Puga
pyp_computers@yahoo.es

Tamaño: 4 KB

Codigo que exporta los datos de unj listview tipo report a microsoft excel

<http://www.mygnet.com/pages/down.php?cod=1622>

Análisis numéricos

Texto 3d

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 2 KB

Texto 3d

<http://www.mygnet.com/pages/down.php?cod=1615>

Numero Primo

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 2 KB
Numero primo
<http://www.mygnet.com/pages/down.php?cod=1606>

Manejo de base datos

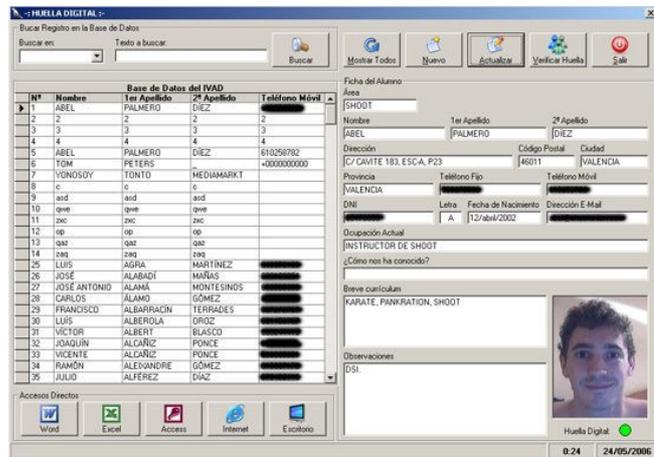
Compacta Y Respalda Base De Datos Protegida Con Contraseña

William Puga
pyp_computers@yahoo.es

Tamaño: 124 B
Solo para bases de datos mdb desde visual basic....
<http://www.mygnet.com/pages/down.php?cod=1667>

Gestión Completa Con Huella Y Fotografía En Mysql

Abel
ab_palmer@hotmail.com



Tamaño: 269 KB
Gestión completa de una bd mysql con huella digital y fotografía.
leer primero el archivo leeme.txt
<http://www.mygnet.com/pages/down.php?cod=1666>

Conexiones Y Tablas En Mysql

Alejandro Benavides
abenavidescr@gmail.com

Tamaño: 829 B
Código fuente para realizar las conexiones con las bases de datos y abrir y cerrar tablas para poder usar estos módulos, se debe activar la referencia: "microsoft activex data objects 2.8 library"
<http://www.mygnet.com/pages/down.php?cod=1645>

Juegos

Codigo De Ajedres

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 90 KB
Codigo fuente de un ajedrez basico, incluye un entorno 100% grafico ademas se maneja desde el muose, maneja modulos de clase y modulos, soporta multiples mejoras, pe; rutinas para fortalecer la defensa etc...
<http://www.mygnet.com/pages/down.php?cod=1625>

Tanques

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 15 KB
Tanques
<http://www.mygnet.com/pages/down.php?cod=1614>

Coches

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 8 KB
Coches
<http://www.mygnet.com/pages/down.php?cod=1612>

Solitario

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 21 KB
Solitario
<http://www.mygnet.com/pages/down.php?cod=1611>

Calculadora

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 7 KB
Calculadora
<http://www.mygnet.com/pages/down.php?cod=1610>

Calendario

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 3 KB
Calculadora
<http://www.mygnet.com/pages/down.php?cod=1609>

Juego De Tetris

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 3 KB
Juego de tetris
<http://www.mygnet.com/pages/down.php?cod=1608>

Calendario

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 28 KB
Calendario
<http://www.mygnet.com/pages/down.php?cod=1605>

Juego Ahorcado

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 92 KB
Juego ahorcado
<http://www.mygnet.com/pages/down.php?cod=1603>

Cálculo y conversiones

Traducir Numeros De Moneda A Letras

Ismael
ismaelignacio82@hotmail.com

Tamaño: 1 KB
Este codigo sirve para leer cantidades monetarias en numeros y traducirlas a letras con el respectivo nombre de la moneda, en mi caso son cordobas
<http://www.mygnet.com/pages/down.php?cod=1660>

Conexiones remotas

Conexion Vb Con Sql

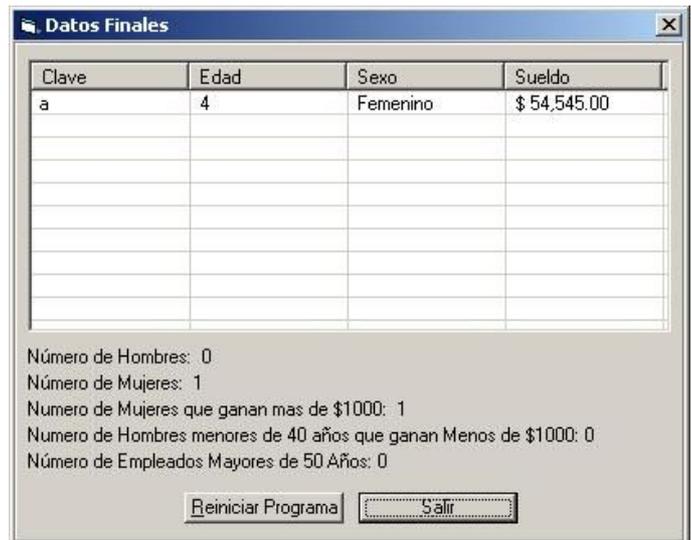
Brejuso
jbreydi@gmail.com

Tamaño: 3 KB
Como hacer una conexión vb con sql
<http://www.mygnet.com/pages/down.php?cod=1655>

Manipulación objetos

Manejo De Arreglos Multi Dimensionales

Lsc Jairo Arturo Segura Morales
lscjairo.segura@gmail.com



Tamaño: 4 KB
Después de estarme quebrando la cabeza un rato con java llegaron unos chicos de la preparatorio iupac para que les hiciera un programita en vb6. los niños querian usar un arreglo que guardara clave, edad, sexo y salario. algo sumamente fácil pero bueno como ellos debe haber mucha gente perdida así que aquí les va este código, realmente muy sencillo. ojalá les sirva de algo
<http://www.mygnet.com/pages/down.php?cod=1597>

Animaciones

Aprende A Haver La Hora

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 3 KB
Aprende a haver la hora como jugfabndo para niños
<http://www.mygnet.com/pages/down.php?cod=1607>

Animacion

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 119 KB
Animacion
<http://www.mygnet.com/pages/down.php?cod=1604>

Graficación

Graficas

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 13 KB
Graficas
<http://www.mygnet.com/pages/down.php?cod=1613>

Virus y troyanos

Keylogger

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 14 KB

Es un muy buen código que un keylog que tiene funciones varias como ejecutar al inicio de windows u ocultarse del ctrl+alt+supr.
<http://www.mygnet.com/pages/down.php?cod=1670>

Crack

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 103 KB

Un buen código fuente para examinar ya que tiene un montón de opciones de email e ip
<http://www.mygnet.com/pages/down.php?cod=1663>

Virus Melissa

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 1 KB

Un virus que fue muy popular años atrás, este código fuente muestra detalladamente el virus melissa
<http://www.mygnet.com/pages/down.php?cod=1658>

Virus Wininet.dll

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 6 KB

El código fuente de un virus que se hace pasar por wininet.dll y cuando es ejecutado este reemplaza al wininet.dll original por uno infectado.
<http://www.mygnet.com/pages/down.php?cod=1657>

Lenguaje Vb.net .net

Numeros Aleatorios Impresos En Excel

Mike
mmayorgah@hotmail.com

Tamaño: 985 KB

Programa que te genera desde 90 a 100 números aleatorios con prueba de varianza y media y que los puedes imprimir en una hoja del excel, los números los puedes pedir entre dos rangos...los que tu quieras.
<http://www.mygnet.com/pages/down.php?cod=1656>

Manejo De Excepciones De Error En Vb.net 2005

Juan Francisco Berrocal
berrocal239@hotmail.com

Tamaño: 18 KB

Aquí muestro como manejar las excepciones en vb.net 2005,

anteriormente en vb6 lo hacíamos con "on error resume next" ahora en .net lo hacemos con trycatch.

<http://www.mygnet.com/pages/down.php?cod=1653>

Registra En Base De Datos

Donald Cornejo Ali
duck7064@hotmail.com

Tamaño: 53 KB

Introduces nombre teléfono, dirección, etc. y todo se almacena en una base de datos
<http://www.mygnet.com/pages/down.php?cod=1623>

Carrera De Autos

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 1 KB

Esta es una carrera de autos esta programado con un timer es bueno mismo lo diseñe
<http://www.mygnet.com/pages/down.php?cod=1600>

Imagenes Chocantes

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 2 KB

Esta es imagen del popular juego de pacman
<http://www.mygnet.com/pages/down.php?cod=1599>

Código Para Convertir De Numeros A Letras

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 2 KB

Este tipo de código es en visual basic.net que sirve para poder ver los números en letras
<http://www.mygnet.com/pages/down.php?cod=1598>

Lenguaje VrmI Multimedia

Planos Xyz En VrmI

Filiberto Ugarte Castañeda
fugartex@hotmail.com

Tamaño: 3 KB

Cuando se diseñan mundos virtuales en vrmI, es necesario tener una referencia espacial para ubicar los nodos y los objetos. es posible desplegar un conjunto de líneas ortogonales separadas un metro entre sí de manera que se obtenga una rejilla o cuadrícula. este código contiene al archivo planos xyz.vrmI para desplegar los 3 planos xy (archivo: plano xy.vrmI), xz (archivo: plano xz.vrmI) y yz (archivo: plano yz.vrmI) con una dimensión de 10 x 10 metros cada uno. convirtiendo en comentario a la línea donde se encuentra el nodo inline del plano deseado evita que sea desplegado.
<http://www.mygnet.com/pages/down.php?cod=1627>

Seguridad informática.

Capítulo 2. Criptología



mygnet@gmail.com

Martin R. Mondragón Sotelo

País: MÉXICO 

Área de estudio: Ing. En Sistemas Computacionales

Experiencia laboral: [2002-2006] Jefe de depto. de sistemas informáticos en la Secretaría de Educación Pública.

Experto en: c++, PHP, VB, Apache

Actividades: Programación de sistemas, Consultoría, Instalaciones y actualizaciones de servidores.

Conocimientos: Administración de servidores.

Diseño de base de datos relacionales. Programación en C++, VC++, c++Builder, Perl, PHP, ASP, VisualBasic, JavaScript, Action Script...

2.1 Servicios de seguridad.

En muchas de nuestras conversaciones de nuestra vida cotidiana hemos utilizado el término seguridad, y que somos expertos en seguridad, que manejamos los firewalls y que creamos, editamos políticas o reglas de seguridad, y que nuestro servidor lo tenemos muy bien protegido. Me pregunto, realmente sabemos que queremos proteger?

Existen servicios y mecanismos de seguridad, pero siempre empezamos por los mecanismos, es decir que utilizamos las herramientas de software de seguridad las cuales instalamos, configuramos y ejecutamos para proteger a nuestro equipo.

Realmente esto es cierto?

Para poder elegir un mecanismo de seguridad primero tengo que definir que es lo que me interesa proteger, es decir que servicios de seguridad necesito.

Antes de utilizar los mecanismos tenemos que tener muy en claro que servicios me interesan.

Los servicios de seguridad son:

- **Autenticación:** Confirmar la identidad de una o mas de las entidades en conexión.
- **Control de acceso:** Protección ante el uso no autorizado de recursos; lectura, escritura, borrado de un archivo en un servidor; ejecución de una rutina o programa.
- **Confidencialidad:** Protección de los datos de difusiones no autorizadas.
- **Integridad de datos:** Garantía de que los campos en los datos transmitidos o almacenados no son modificados, borrados o reproducidos.
- **No repudio (No-rechazo):** Asociar la identidad de un individuo con su participación en un proceso. Esto es útil para probar que un mensaje fue generado por un usuario concreto.
- **Gestión de seguridad:** Administrar la directiva global de seguridad, los mecanismos de seguridad específicos (por ejemplo, las claves criptográficas, los mecanismos de autenticación y otros mecanismos de control), los sucesos de seguridad, las auditorías de seguridad y la restauración de la seguridad.

Dependiendo de nuestras necesidades de seguridad podremos hacer un análisis donde la combinación de servicios y mecanismos nos ofrezca alternativas de superación para estas necesidades.

2.1.1 Autenticación.



combinación de mecanismos.

La autenticación (también conocida como "identificación" conlleva la confirmación de las identidades de una o más entidades. En general, puedes considerar la autenticación como el identificarte ante un sistema, subsistema, red o aplicación, mediante algún mecanismo o

Mecanismos:

- **Nombre de usuario y contraseña** (criptografía)
- **Tickets de acceso:** Son identificadores temporales que son solicitados por el cliente a un servidor.
- **Certificados digitales:** Es como una credencial la cual incluyen información estandarizada como la clave pública del propietario, nombre, fechas de caducidad, firma de una autoridad certificadora, entre otros datos.
- **Tarjetas inteligentes:** Pueden contener claves privadas, certificados digitales u otra información sobre la entidad. También pueden tener una protección mediante un número de identificación personal.
- **Tokens (Fichas):** Las tarjetas Token están protegidas por pin o por otro mecanismo, como la generación de números mediante los token de seguridad. Estos números son conocidos por la tarjeta y el servidor de autenticación.
- **Dispositivos biométricos:** Estos dispositivos realizan análisis estadísticos de patrones generados analizando una parte de una persona (retina, iris, rostro, huella dactilar, voz, etc.) para establecer una identificación personal.

2.1.2 Control de acceso



Mediante el control de acceso se protege el uso no autorizado de los recursos. Generalmente, hay un orden implícito, según el cual una entidad primero se identifica y autentica, y a continuación se le proporciona el acceso o se le deniega. Cada entidad tiene sus permisos de acceso a cada recurso especificado.

Mecanismos:

- **Listas de control de acceso:** Una lista de entidades, junto a sus permisos de acceso, que tienen autorización para acceder al recurso.
- **Etiquetas de seguridad:** Una colección de atributos asociados con una entidad que permiten la clasificación de la entidad en términos de nivel de seguridad.
- **Roles o privilegios:** Un atributo de privilegio que representa la posición o función que representa un usuario que busca una autenticación. Un determinado ser humano puede soportar diversos roles y de este modo requerir muchos atributos de privilegio.
- **Barreras físicas:** El acceso físico a dispositivos del sistema y la red debe limitarse mediante habitaciones cerradas

mediante llaves, contraseñas u otros mecanismos de control de accesos, pueden ser de 1 a 3 perímetros.

- **Firewalls:** Son funciones de filtrado y Proxy pueden evitar el acceso a determinados recursos o direcciones de la red.

2.1.3 Confidencialidad



La confidencialidad consiste en proteger los datos transmitidos o almacenados que no puedan ser leídos por un tercero no autorizado. Podemos implementar varios algoritmos criptográficos para proporcionar la confidencialidad.

Sabemos que las redes no fueron echas tomando en cuenta el paradigma de seguridad y no es confiable transmitir la información ya que la información viaja en texto claro y son interceptada por terceros. Pero las necesidades de enviar información nos obliga a buscar soluciones seguras como la criptografía de datos de tal forma que aunque la información sea interceptada no puedan saber cual es el mensaje.

Mecanismos:

- **Criptografía:** proporciona niveles más altos de confidencialidad ya que el mensaje no viaja en claro.
- **Esteganografía:** Consiste en ocultar un mensaje de secreto en otro mensaje que aparece normal. Ha sido utilizado en el pasado, antes de la llegada de los ordenadores y las redes. Hoy en día a veces se utilizan en conjunto con la criptografía.

2.1.4 Integridad de Datos



Consiste en impedir que los datos almacenados o transmitidos sean modificados, borrados o reproducidos.

Mecanismos:

- **Checksums:** Es un número que representa la suma de bloques del mensaje que se envía junto con este, y al ser recibido el mensaje se calcula el checksums y se compara con el que se recibió y si son iguales quiere decir que el mensaje no fue alterado. Este sencillo mecanismo de integridad de datos puede ser falsificado muy fácilmente.

Por ejemplo. M es un mensaje puede ser interceptado y modificado de modo que se transmita un M distinto al que se envió, y además se cambia el checksums que al ser recibido el destino no se da cuenta que fue alterado, y da por hecho que es íntegro.

- **Control de redundancia cíclica:** Consiste en una transmisión de datos que se divide en paquetes. El emisor adjunta una secuencia de n-bits llamada secuencia de control de paquete a cada paquete. El control de paquete contiene

información redundante sobre el paquete que permite al receptor detectar errores en dicho paquete, también existe un escenario de ataque.

- **Resúmenes de mensajes.** Un resumen de mensaje es una cadena de bits que fue calculado utilizando el mensaje como datos de entrada en una función de resumen en un solo sentido. Llamamos también hash unidireccional que es fácil de procesar en un sentido pero imposible invertir. Esto quiere decir que es imposible llegar al mensaje original a partir de un hash. También es dos o más mensajes no pueden tener el mismos hash.

Un ejemplo de implementación de los hash en un antivirus, algunos de estos calculan el hash para comprobar si los archivos han sido alterados o corruptos.

2.1.5 No-rechazo o No-repudio



El no-repudio pretende demostrar la participación de un individuo en el cual un proceso se relacione con la identificación de este, en otras palabras un emisor tienen la forma de garantizar que el receptor no repudiara el mensaje donde el repudio consiste en negar la autoría sobre un mensaje.

Uno de los mecanismos que se utilizan para este servicio es la certificado digital en otras palabras firma digital. También se pueden utilizar funciones hash.

Pueden existen mas servicios de seguridad, esto va depender de la políticas de la empresa u organización.

Ya tenemos nociones básicas de los servicios de seguridad, algo que tienen que quedar claro es que no se pueden garantizar todos a un 100%, hay que hacer un análisis de que es los que mas le interesa a la empresa, claro también hay que contemplar los costos, por que quizás me interese integridad y no confidencialidad o viceversa o ambas.

La mayoría de estos servicios de seguridad pueden utilizar la criptografía como mecanismos para cumplir con estos.

2.2. Criptología.

Proviene del griego: *criptos* (oculto) y *logos* (tratado). Es la ciencia que oculta la información.

Es el estudio de los criptosistemas: sistemas que ofrecen medios seguros de comunicación en los que el emisor oculta o cifra el mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo.

La criptología se puede dividir en 3 áreas: *Criptografía*, *Criptoanálisis* y *Esteganografía*.

Criptografía

La criptografía (del griego *kryptos*, "ocultar", y *grafos*, "escribir",

literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Criptoanálisis.

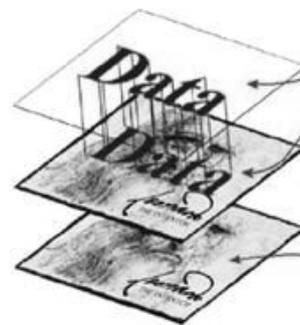
Es la técnica para descifrar la información sin conocer la llave de cifrado. La más famosa es sin duda la que aplicaron a Enigma de los Nazis tras dos años de investigación pero las técnicas fueron evolucionando hasta la biometría criptográfica.



La máquina Enigma era un mecanismo de cifrado rotativo utilizado tanto para cifrado como para descifrado, ampliamente utilizada de varios modos en Europa desde los tempranos años 1920 en adelante. Su fama se la debe a haber sido adoptada por muchas fuerzas militares de Alemania desde 1930 en adelante. Su facilidad de manejo y su supuesta inviolabilidad fueron las principales razones para su amplio uso. Su cifrado, fue roto, y la lectura de la información que ofrecía en los mensajes que no protegió es a veces reconocida como la causa para acabar al menos un año antes la Segunda Guerra Mundial de lo que hubiera podido ser de otro modo.

Esteganografía

Área de la criptología que trata sobre la ocultación de mensajes, para evitar que se perciba la existencia del mismo. Viene del griego *stegos* (ocultar) y *graphia* (escritura).



Es el arte y ciencia de escribir mensajes ocultos de tal forma que nadie fuera de quien lo envía y quien lo recibe sabe de su existencia.

El problema de la esteganografía es que tienen que mantener en secreto el algoritmo de ocultamiento a diferencia de la criptografía donde se conoce el algoritmo.

Los mensajes en la esteganografía muchas veces son cifrados primero por medios tradicionales, para posteriormente ser ocultados.

2.2.1 Criptografía.

Es un método que convierte un mensaje (Texto en claro) en un mensaje cifrado (Texto secreto).

Conceptos:

Texto en claro: es mensaje en su forma natural lo que se debe proteger.

Texto cifrado: Es el proceso de convertir el texto en claro en un texto ilegible, también denominado como texto cifrado o criptograma.

Sustitución. Cambiar elementos (letras, dígitos y símbolos) por otros del mensaje de acuerdo a un alfabeto.

Transposición. Reordenación de los elementos del mensaje.

Producto: Combinación de sustitución y transposición.

Monoalfabeto. Un solo alfabeto.

Polialfabeto. Dos o más alfabetos.

La criptografía se clasifica en clásica y moderna.

2.2.1.1 criptografía clásica.

Las dos técnicas más básicas de cifrado en la criptografía clásica son la sustitución (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la transposición (que supone una reordenación de las mismas); la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas. El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave.

Algunos algoritmos de la criptografía clásica por sustitución monoalfabéticas:

Código de Políbio

El historiador griego Políbio (204 la.C. la 122 la.C.), en su libro Historias, describe un ejemplo muy antiguo de un código poligrámico, que es atribuido a sus contemporáneos Cleoxeno y Democleto.

El alfabeto griego sólo posee 24 letras. Políbio proponía que la 25ª. Posición (vaga) fuera utilizada como señal de sincronización - inicio y fin de la transmisión. En el ejemplo abajo se utiliza el alfabeto latino que, por su parte, posee el "defecto" de poseer 26 letras. De este modo, para obtenerse la cifra, los caracteres K y Q, raros, sin embargo fonéticamente muy próximos, fueron "fundidos".

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K/Q	L	M	N	O
4	P	R	S	T	U
5	V	W	X	Y	Z

Cada letra es representada por la combinación de dos números, los cuales se refieren a la posición ocupada por la letra. De esta forma, A es sustituido por 11, B por 12..., L por 32, etc.

El código de Políbio tiene algunas características importantes: la reducción del número de caracteres utilizados, la conversión en números y la transformación de un símbolo en dos partes que pueden ser usadas separadamente. Su importancia en la historia de la criptografía reside en el hecho de que sirvió de base para otros códigos de cifragem, como la Cifra Playfair y la Cifra Campal Germánica (ADFGFX), usada en la

Por ejemplo:

Texto en claro: MYGNET
 Texto cifrado: 335422342544

Criptoanálisis.

El ataque para este criptosistema es por el Análisis de Frecuencia.

Cifrado César.

Utilizado por Julio César para comunicarse con sus oficiales, consiste en sustituir cada letra del mensaje por la que está k posiciones más adelante o atrás en el alfabeto de N caracteres. Si $k = 3$, la A se sustituiría por la D, la B por E, la C por la F y así sucesivamente.

Por ejemplo:

Para: $K = 3$
 Texto en claro: MYGNET
 Texto Cifrado: PBJQHW

Criptoanálisis.

El ataque para este criptosistema es por el Análisis de Frecuencia.

Código fuente en php:

```
<?php
function cifrar($M,$k)
{
    for($i=0; $i<strlen($M);
    $i++)$C.=chr((ord($M[$i])+$k)%255);
    return $C;
}
function decifrar($C,$k)
{
    for($i=0; $i<strlen($C); $i++)$M.=chr((ord($C[$i])-
    $k+255)%255);
    return $M;
}
//Ejemplo de cifrado y de descifrado...
$mensaje="Este es un mensaje super secreto!...";
$c=cifrar($mensaje,3); //Cifrar
$m=decifrar($c,3); //Descifrar
echo $mensaje.' <=> '.$c.' <=> '.$m;
?>
```

Cifrado del Kama-Sutra

Una de las descripciones más antiguas de encriptación por sustitución está en el Kama-Sutra, un texto escrito el siglo IV d.C. por el sabio hindú Vatsyayana, sin embargo basado en manuscritos datados de más de 800 años (séc. IV a.C.). El Kama-Sutra recomienda que las mujeres estudien 64 artes, incluyendo la culinaria, la forma de vestir, masaje y la preparación de perfumes.

La lista también incluye algunos artes menos obvios como prestidigitación, ajedrez, encuadernación de libros y carpintería. En la lista, la de número 45 es la mlecchita-vikalpa, el arte de la escritura secreta, indicada para ayudar las mujeres a esconder los detalles de sus relaciones. Una de las técnicas recomendadas es la de formar pares aleatorios de letras del alfabeto y después sustituir cada letra del texto original por la correspondiente en el par.

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

Por ejemplo:

Texto en claro: MYGNET LA COMUNIDAD
 Texto cifrado: CPISUZ RV MQCESGXVX

Criptoanálisis:

Escenario de ataque: análisis de frecuencias.

Código fuente en php

```
<?php
$ALFABETO=array( array('A','D','H','I','K','M','O','R','S','U','W','Y','Z'),
  array('V','X','B','G','J','C','Q','L','N','E','F','P','T')
);

function kama($TXT,$ALFABETO)
{ $TMP=array();
  for($i=0; $i<count($ALFABETO[0]); $i++)
  { $TMP[$ALFABETO[0][$i]]=$ALFABETO[1][$i];
    $TMP[$ALFABETO[1][$i]]=$ALFABETO[0][$i];
  }
  $result = "";
  for($i=0; $i<strlen($TXT);
  $i++)$result.=isset($TMP[$TXT[$i]])?$TMP[$TXT[$i]]:' ';
  return $result;
}

$dd=kama('MYGNET LA COMUNIDAD',$ALFABETO);
echo $dd.' == '.kama($dd,$ALFABETO);
?>
```

Algunos algoritmos de la criptografía clásica por sustitución

Polialfabética:

Cifrado PlayFair

Desarrolle este algoritmo con fines didácticos, ya que solo soporta 25 caracteres los cuales son muy pocos, aunque se podrían hacer implementaciones con más caracteres basándose en este algoritmo pero dejaría de ser el cifrado de playfair.

Este sistema criptográfico fue inventado en 1854 por Charles Wheatstone, pero debe su nombre al Barón Playfair de St Andrews quien promovió el uso de este criptosistema.

El algoritmo utiliza una tabla o matriz de 5x5.

La tabla se llena con una palabra o frase secreta descartando las letras repetidas. Se rellenan los espacios de la tabla con las letras del alfabeto en orden. Usualmente se omite la "W" y se utiliza la "V" en su lugar o se reemplazan las "J" por "I". Esto se hace debido a que la tabla tiene 25 espacios y el alfabeto tiene 26 símbolos. La frase secreta usualmente se ingresa a la tabla de izquierda a derecha y arriba hacia abajo o en forma de espiral, pero puede utilizarse algún otro patrón. La frase secreta junto con las

convenciones para llenar la tabla de 5x5 constituye la clave de encriptación.

Criptoanálisis:

Análisis de frecuencia de dígrafos. Por ser una cifra polialfabética, la Playfair dificulta el criptoanálisis. Por ser una cifra de dígrafos, es preciso hacer un análisis de frecuencia de dígrafos - y existen más dígrafos que letras - y el número de elementos disponibles para análisis disminuye. Por ejemplo: en un mensaje de 100 letras, cifrada con una sustitución simple, tenemos 100 elementos derivados de una elección de 26; en un mensaje de 100 letras, cifrada en dígrafos, tenemos 50 elementos derivados de una elección de 676.

Código fuente en php:

```
<?php
//Tabla del alfabeto...
$T=array();
$Tp=array();
function buscar($s,$c=true)
{ global $Tp;
  for($i=0; $i<5; $i++)for($j=0;$j<5; $j++) if($Tp[$i][$j]==$s)
  return $c?$i:$j;
  return false;
}
function setcar($s)
{ global $T;
  if(trim($s)!="){ for($i=0; $i<count($T); $i++)if($T[$i]==$s){
  $T[$i]=""; return $s; } return ""; }
  for($i=0; $i<count($T); $i++)if($T[$i]!="){ $s=$T[$i]; $T[$i]="";
  return $s; }
}
function matrizTp($K)
{ global $Tp,$T;
  $Tp=array();
  $T=array(
  'A','B','C','D','E',/**/
  'F','G','H','I','J',/**/
  'K','L','M','N','O',/**/
  'P','Q','R','S','T',/**/
  'U','V','X','Y','Z');

  $K=str_replace('W','V',strtoupper($K)); $n=0;
  for($i=0; $i<5; $i++)
  { for($j=0;$j<5; $j++)
  { do{ $Tp[$i][$j]=setcar($K[$n++]);
  }while($Tp[$i][$j]=="");
  }
  }
}
function playfair($M,$K)
{ global $Tp;
  matrizTp($K);
  $M=str_replace('W','V',strtoupper($M));
  for($i=0; $i<strlen($M); $i+=2)
  { $C.= $Tp[buscar($M[$i],true)][buscar($M[$i+1],false)].
  $Tp[buscar($M[$i+1],true)][buscar($M[$i],false)];
  }
}
```

```
return $C;
}
/* Ejemplo..*/
$K='comunidad'; //Clave
$M='lenguaje';
$C=playfair($M,$K);

echo '<code>Algoritmo de Playfair<hr>';
echo 'Clave: '.$K.'<hr>';
echo 'Cifrado: '.$C.'<hr>';
for($i=0; $i<5; $i++)
{ echo '<br>';
  for($j=0;$j<5; $j++) echo $Tp[$i][$j].' ';
} echo '<hr>';
$M=playfair($C,$K);
echo 'Decifrado: '.$M.'</code><hr>';
?>
```

Cifrado de Vigenère

En el quinto volumen de sus seis libros titulados Polygraphiae, Jean Trithème describe una tabla que se imaginó y nombrada tabulò recta. En esta tabla, el alfabeto se repite en 26 líneas, con un desfase a la izquierda de una letra para cada nueva hilera.

El diplomático francés Blaise de Vigenère, que vivió de 1523 a 1596, usó la criptografía como instrumento de trabajo durante años. Con la edad de 39 años resolvió abandonar la carrera y dedicarse exclusivamente a los estudios.

En 1586, Blaise de Vigenère reanuda esta idea en su libro de criptología, el *Traité des chiffres où secrètes manières d'escrire*, en el cual describe detalladamente su cifra de sustitución polialfabética con palabra-llave y presenta las Carreras de

Vigenère, una tabla de alfabetos cifrantes.

El gran mérito de Vigenère está en perfeccionar un método que ya había sido propuesto por otros estudiosos, pero que necesitaba ser estructurado para ofrecer la seguridad necesaria. Vigenère se basó en Alberti y Trithemius, como también en algunos contemporáneos, como Bellaso y Della Puerta.

La denominación calcula de Vigenère apareció solamente al final del siglo XVII, en el honor de el que le dio su forma definitiva. Sin embargo el término cuadrado de Vigenère es erróneo, se debería más bien decir cuadrado de Trithème.

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

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

La clave del sistema de cifrado de Vigenère es una palabra de letras, del alfabeto utilizado anteriormente; esta palabra es un elemento del producto cartesiano (veces), que es justamente el alfabeto del criptosistema de Vigenère. De esta forma, el mensaje a cifrar en texto claro ha de descomponerse en bloques de elementos - letras - y aplicar sucesivamente la clave empleada a cada uno de estos bloques, utilizando la tabla anteriormente proporcionada.

Por ejemplo:

```
Clave: clave
Texto en claro: COMUNIDAD MYGNET
Texto cifrado: EZMPRKOAY OJGIIV
```

Criptoanálisis:

Método de Kasiski/Babbage, Índice de Coincidencia (IC) o ambos asociados.

En 1863 que el criptólogo alemán Kasiski descubrió como quebrar la cifra de Vigenère. El matemático inglés Charles Babbage ya había quebrado la cifra en 1854, sin embargo no publicó su descubrimiento.

Código fuente en php:

```
<?php
function vige($texto,$clave,$ty=true)
{ $alfabeto = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
  $texto=strtoupper($texto);
  $clave=strtoupper($clave);
  $cla=$clave;
  while(strlen($clave)<strlen($texto))$clave.=$cla;
  $result= "";
  for($i=0; $i< strlen($texto); $i++)
  { if($texto[$i]!=' '){ $result.=$texto[$i]; continue; } }
```

```

$idx = strpos($alfabeto,$texto[$i]);
if($idx < 0) $result .= $texto[$i];
else {
    $k = strpos($alfabeto,$clave[$i]);
    $idx+=$ty?$k:strlen($alfabeto)-$k;
    $result.=$alfabeto[$idx % strlen($alfabeto)];
}
}
return $result;
}

function cifrado($texto,$clave){ return vige($texto,$clave,true); }
function decifrado($texto,$clave){ return
vige($texto,$clave,false); }

$dd=cifrado('comunidad mygnet','clave');
echo $dd.' == '.decifrado($dd,'clave',false);
?>

```

Existen muchos mas critosistemas clásicos...

2.2.1.2 Criptografía moderna:

Los modernos algoritmos de cifrado simétricos mezclan la transposición y permutación en cuanto a los algoritmos asimétricos se basan en complejas operaciones matemáticas a lo que se le conoce como logaritmo discreto.

En los sistemas de encriptación se suele distinguir entre el algoritmo o procedimiento general y la clave, que sirve para singularizar el resultado del algoritmo. En el caso del cifrado César, el algoritmo sería la regla por la cuál cambiamos cada carácter por uno que está N posiciones más adelante, mientras que la clave sería el valor concreto utilizado para N.

Lo malo de este sistema es que, si se sabe que se está utilizando, solo permite 27 sustituciones distintas (tantas como letras tienen el alfabeto), con lo que su descifrado es trivial. Para complicar un poco mas se puede utilizar, en vez de una cifra, dos, o más. Así, si la clave es 31, se sustituirá la primera letra por la que esté tres posiciones por delante, la segunda por la que esté una posición más avanzada, la tercera por la que esté tres posiciones por delante, y así sucesivamente.

2.2.1.2.1 Criptografía simétrica.

Este tipo de criptografía utiliza la misma clave para cifrar y para descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.



Toda la seguridad esta basada en la llave que comparten el emisor y el receptor los cuales deben mantenerla en secreto por que si la llave se compromete el sistema deja de ser seguro.

Existen muchos algoritmos de llave simétrica, aquí vamos a mencionar 2, DES por ser el algoritmo mas utilizado aunque en la actualidad no es recomendable su implementación, y AES es relativamente nuevo y es el que sustituye a DES.

Tienen ventajas como desventajas.

Es muy rápido en cuestiones de procesamiento.

Uno de los problemas de este tipo de criptografía es el acuerdo de la llaves, es un problema que se puede expresar de la siguiente manera: $N(N-1)/2 \Rightarrow (N^2 - N)/2$ es una ecuación exponencial donde N es el numero de partes o nodos que tienen que compartir las llaves. Esta ecuación devuelve el número de envíos que se tienen que hacer para compartir la llave simétrica.

Algoritmo DES.

Data Encryption Standard (DES) es un algoritmo para cifrar un mensaje, escogido como FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis.

Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto; las claves de DES se han roto en menos de 24 horas. Existen también resultados analíticos que demuestran debilidades teóricas en su cifrado, aunque son inviables en la práctica. Se cree que el algoritmo es seguro en la práctica en su variante de Triple DES, aunque existan ataques teóricos.

Desde hace algunos años, el algoritmo ha sido sustituido por el nuevo AES (Advanced Encryption Standard).

DES es el algoritmo prototipo del cifrado por bloques — un algoritmo que toma un texto en claro de una longitud fija de bits y lo transforma mediante una serie de complicadas operaciones en otro texto cifrado de la misma longitud. En el caso de DES el tamaño del bloque es de 64 bits. DES utiliza también una clave criptográfica para modificar la transformación, de modo que el descifrado sólo puede ser realizado por aquellos que conozcan la clave concreta utilizada en el cifrado. La clave mide 64 bits, aunque en realidad, sólo 56 de ellos son empleados por el algoritmo. Los ocho bits restantes se utilizan únicamente para comprobar la paridad, y después son descartados. Por tanto, la longitud de clave efectiva en DES es de 56 bits, y así es como se suele especificar.

Al igual que otros cifrados de bloque, DES debe ser utilizado en el modo de operación de cifrado de bloque si se aplica a un mensaje mayor de 64 bits. FIPS-81 especifica varios modos para el uso con DES, incluyendo uno para autenticación. Se pueden consultar más

documentos sobre el uso de DES en FIPS-74 <http://www.itl.nist.gov/fipspubs/fip74.htm>

Criptoanalisis:

Como para cualquier tipo de cifrado se puede realizar ataques por fuerza bruta.

Existen otros ataques conocidos que pueden romper las dieciséis rondas completas de DES con menos complejidad que un ataque por fuerza bruta: el criptoanálisis diferencial (CD), el criptoanálisis lineal (CL) y el ataque de Davies. De todas maneras, éstos ataques son sólo teóricos y no es posible llevarlos a la práctica; éste tipo de ataques se denominan a veces debilidades certificacionales.

- *El criptoanálisis diferencial* fue descubierto a finales de los 80 por Eli Biham y Adi Shamir, aunque era conocido anteriormente tanto por la NSA como por IBM y mantenido en secreto. Para romper las 16 rondas completas, el criptoanálisis diferencial requiere 247 textos planos escogidos. DES fue diseñado para ser resistente al CD.
- *El criptoanálisis lineal* fue descubierto por Mitsuru Matsui, y necesita 243 textos planos escogidos (Matsui, 1993); el método fue implementado (Matsui, 1994), y fue el primer criptoanálisis experimental de DES que se dio a conocer. No hay evidencias de que DES fuese adaptado para ser resistente a este tipo de ataque. Una generalización del CL — el criptoanálisis lineal múltiple — se propuso en 1994 (Kaliski and Robshaw), y fue mejorada por Biryukov y otros (2004); su análisis sugiere que se podrían utilizar múltiples aproximaciones lineales para reducir los requisitos de datos del ataque en al menos un factor de 4 (es decir, 241 en lugar de 243). Una reducción similar en la complejidad de datos puede obtenerse con una variante del criptoanálisis lineal de textos planos escogidos (Knudsen y Mathiassen, 2000). Junod (2001) realizó varios experimentos para determinar la complejidad real del criptoanálisis lineal, y descubrió que era algo más rápido de lo predicho, requiriendo un tiempo equivalente a 239–241 comprobaciones en DES.
- *El ataque mejorado de Davies*: mientras que el análisis lineal y diferencial son técnicas generales y pueden aplicarse a multitud de esquemas diferentes, el ataque de Davies es una técnica especializada para DES. Propuesta por vez primera por Davies en los 80, y mejorada por Biham and Biryukov (1997). La forma más potente del ataque requiere 250 textos planos escogidos, tiene una complejidad computacional de 250, y tiene un 51% de probabilidad de éxito.

Algoritmo AES.

Advanced Encryption Standard (AES), también conocido como Rijndael, es un esquema de cifrado por bloque adoptado como un estándar de encriptación por el gobierno de los Estados Unidos, y se espera que sea usado en el mundo entero, como también analizado exhaustivamente, como fue el caso de su predecesor, el Estándar de Encriptación de Datos (DES). Fue adoptado por el Instituto Nacional de Estándares y Tecnología (NIST) como un FIPS (PUB 197) en noviembre del 2001 después de 5 años del proceso

de estandarización (vea Advanced Encryption Standard process para más detalles).

Estrictamente hablando, AES no es precisamente Rijndael (aunque en la práctica se lo llama de manera indistinta) ya que Rijndael permite un mayor rango de tamaño de bloque y clave; AES tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 ó 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits.

La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado.

AES opera en un arreglo de 4×4 bytes, llamado state (algunas versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en el state). Para el cifrado, cada ronda de la aplicación del algoritmo AES (excepto la última) consiste en cuatro pasos:

- **SubBytes**: en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla lookup table.
 - **ShiftRows**: en este paso se realiza una transposición donde cada fila del state es rotado de manera cíclica un número determinado de veces.
 - **MixColumns**: operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.
 - **AddRoundKey**: cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una key schedule.
- La ronda final omite la fase MixColumns.

Criptoanalisis:

En abril de 2005, D.J. Bernstein anunció a Ataque temporizado de cache que solía romper un servidor a medida que usaba el cifrado AES para OpenSSL. Este servidor fue diseñado para dar la mayor cantidad de información acerca del tiempo como fuera posible, y el ataque requería cerca de 200 millones de ficheros de texto plano. Se dice que el ataque no es práctico en implementaciones del mundo real.

2.2.1.2.2 Criptografía asimétrica.

Este método consiste en generar una pareja de llaves, una pública y privada, se cifra con una y se descifra con la otra. La llave pública se puede entregar a cualquier persona y la clave que es privada se tienen que mantener en secreto y que nadie excepto el propietario tenga acceso a esta llave. Si se compromete la llave privada se tienen que generar otra pareja de llaves, pues las llave privada y la pública son totalmente dependientes una de la otra.

El concepto de llave pública apareció en el 1976 en un artículo debido a *Diffie-Hellman*

La criptografía asimétrica es costosa y requiere mucho procesamiento, no es recomendable cifrar mensajes grandes, se

utiliza comúnmente para acordar las llaves simétricas, a este tipo de sistemas criptográficos se les conoce también como criptografía híbrida.



Aquí se reduce el problema de compartir la llave a polinomialmente, en vez de exponencial como era el caso de la criptografía simétrica, pero el problema aquí es autenticar las llaves públicas, ya que no hay garantía que el receptor reciba íntegra la llave pública o peor a un, que sea la llave de un impostor, y con esto nace todo lo que ya conocemos como certificados digitales, que certifican a las llaves públicas como genuinas y que pertenecen a una entidad, para esto debe de existir una tercera parte confiable que son las autoridades certificadoras.

Pero no vamos a entrar muchos en detalles ya que se va hablar un capítulo de todo esto de los certificados digitales.

Y como algoritmo vamos a ver el RSA para criptografía asimétrica..

Algoritmo RSA.

El sistema criptográfico con clave pública RSA recibe su nombre por la inicial del apellido de sus inventores: Ronald Rivest, Adi Shamir y Leonard Adleman. Todo usuario de dicho sistema hace pública una clave de cifrado y oculta una clave de descifrado. Una llave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes. Cuando se envía un mensaje, el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. La seguridad de este algoritmo radica en que no hay maneras rápidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales. La computación cuántica podría proveer una solución a este problema de factorización.

Los conocimientos necesarios para entender el RSA son básicos. Ante todo, es preciso acordarse que un número primo es un número diferente de 1 que sólo es divisible exactamente por 1 o por sí mismo. Así, 3 es un número primo porque sólo tiene una división exacta cuando dividido por 1 o por 3. Ya el número 4 no es primo porque puede ser dividido exactamente por 1, 2 y 4. Si el número 4 no es un número primo, entonces puede ser factorizado, o sea, puede encontrarse los números primos que, multiplicados, resultan 4 (en el caso, 2×2).

Existen algunos números conocidos como primos entre sí. Dos números enteros son primos entre sí cuando no

existe un divisor mayor que 1 que divida ambos. Esto significa que el máximo divisor común de los primos entre sí es igual a 1.

x	1.	2.	3.	4.	5.	6.
3x	3.	9.	27.	81.	243.	729.
3x (mod 7)	3.	2.	6.	4.	5.	1.
Comportamiento errático de la función 3x (mod 7)						

Otro concepto necesario es la aritmética modular. En la aritmética modular no disponemos de una cantidad infinita de números, pero de un grupo finito de ellos. El mejor ejemplo es el mostrado por el reloj que, por señal, trabaja en el módulo 12. Cuando la esfera pasa del 12, no tiene como mostrar 13 horas porque el conjunto de los números disponibles va de 1 a 12. De esta forma, $12 \text{ horas} + 1 \text{ hora} = 1$ y $9 \text{ horas} + 8 \text{ horas} = 5$. Se suele escribir estas operaciones de la siguiente forma: $12 + 1 = 1 \pmod{12}$ y $9 + 8 = 5 \pmod{12}$.

El modo de encontrarse un resultado modular es dividiendo el resultado no modular por el módulo y considerar el resto. Por ejemplo, $9 + 8 = 17$ y $17 \div 12 = 1$ con resto 5. De la misma forma, $11 \times 9 \pmod{13}$ es $11 \times 9 = 99$ y $99 \div 13 = 7$ con resto 8, o sea, $11 \times 9 = 8 \pmod{13}$. Podemos complicar un poco las cosas y considerar una potenciación. Digamos que la base sea 3 y que este número sea elevado a un número cualquiera que llamaremos de x. Para analizar el comportamiento de la función $3x \pmod{7}$ acompañe los resultados obtenidos en la tabla 1. En la operación normal, los valores encontrados son crecientes. Ya en la operación modular, los resultados son erráticos y difíciles de predecir.

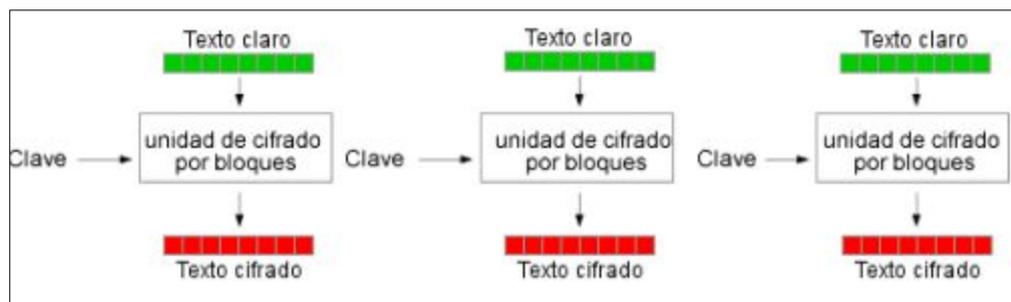
2.2.1.3 Criptografía por modo de operación:

La criptografía por modo de operación puede ser de flujo o de bloque. Las de bloque operan en bloques de tamaño fijo, generalmente de 64 o 128 bits. Los primeros son flujos de datos se producen en tiempo real en pequeños fragmentos, donde las muestras de datos pueden ser tan pequeñas como 8 bits o incluso de 1 bit, y sería un desperdicio rellenar el resto de los 64 bits antes de cifrar y transmitirlos.

La mayoría sólo son utilizados para la confidencialidad; algunas proporcionan confidencialidad y autenticación.

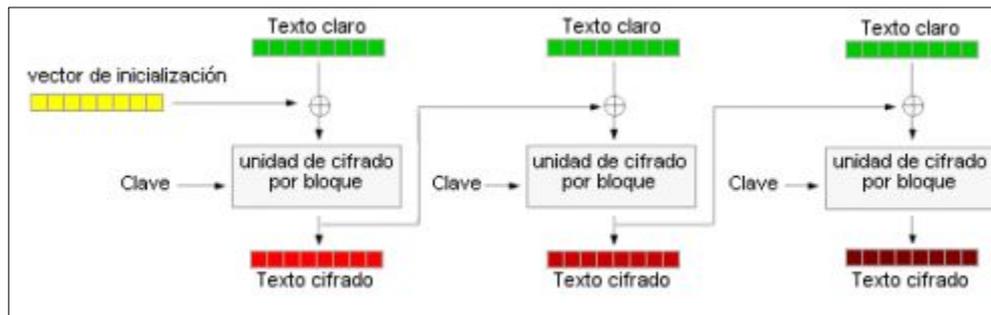
ECB - Electronic codebook

El más sencillo de los modos de uso es el modo electrónico codebook (ECB), en el cual los mensajes se dividen en bloques y cada uno de ellos es cifrado por separado. La desventaja de este método es que a bloques de texto en claro idénticos les corresponde bloques idénticos de texto cifrado, de manera que se pueden reconocer estos patrones como guía para descubrir el texto en claro a partir del texto cifrado. De allí que no sea recomendado para su uso en protocolos cifrados.



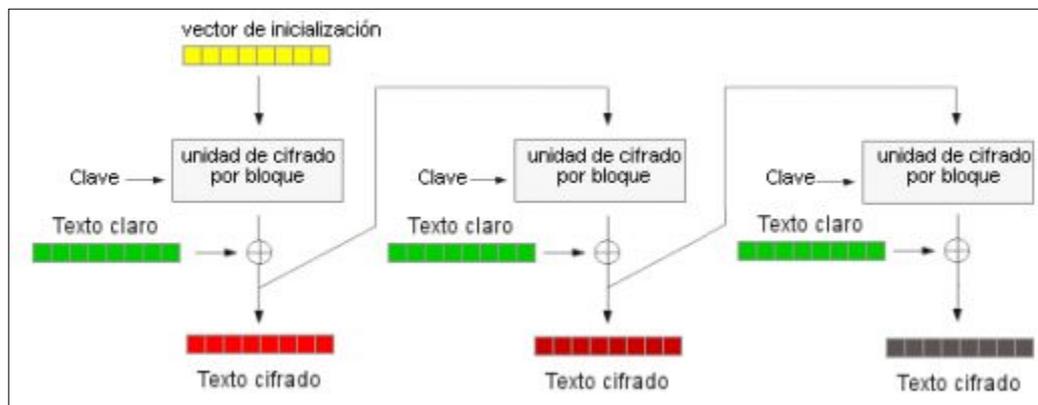
CBC - Cipher-block chaining

En el modo cipher-block chaining (CBC), a cada bloque de texto en claro se le aplica la operación XOR con el bloque cifrado anterior antes de ser cifrado. De esta forma, cada bloque de texto cifrado depende de todo el texto en claro procesado hasta este punto. También, para hacer cada mensaje único se utiliza un vector de inicialización. Su mayor desventaja es que es secuencial. Como no puede ser usado en paralelo (pues siempre depende del resultado anterior), su uso dificulta el procesamiento de bloques en paralelo, lo que mejoraría el desempeño del método.



CFB - Cipher feedback y OFB - output feedback

Los modos cipher feedback (CFB) y output feedback (OFB) hacen que el cifrado en bloque opere como una unidad de flujo de cifrado: se generan bloques de flujo de claves, que son operados con XOR y el texto en claro para obtener el texto cifrado. Al igual que con otras unidades de flujo de cifrado, al intercambiar un bit en el texto cifrado produce texto cifrado con un bit intercambiado en el texto en claro en la misma ubicación.



Con el cipher feedback un bloque de flujo de llave es calculado cifrándose el bloque de texto cifrado anterior.

Counter (CTR)

Al igual que OFB, el modo contador convierte una unidad de cifrado por bloques en una unidad de flujo de cifrado. Genera el siguiente bloque en el flujo de claves cifrando valores sucesivos de un contador. El contador puede ser cualquier función sencilla que produzca una secuencia de números donde los resultados se repiten con muy baja frecuencia, si bien la operación más usada es un contador, el modo CTR tiene características similares al OFB, pero permite también el uso de una propiedad de acceso aleatorio para el descifrado.

Desventaja es que no proporcionan cualquier protección de integridad. Esto significa que un atacante, a pesar de no conocer la llave, puede modificar el flujo de datos de acuerdo con sus necesidades.

2.2.2 Esteganografía.

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 el contenido del mensaje está oculto. 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, la gente escribía mensajes en una tabla de madera y después la cubrían con cera para que pareciera que no había sido usada.
- 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.

Aquí esta un artículo sobre un ejemplo práctico de esteganografía en una imagen.: <http://www.mygnet.com/articulos/php/448/>

2.2.3 Criptoanálisis.

Es la ciencia que trata principalmente de crear y analizar criptosistemas seguros, se intenta romper esos sistemas, demostrando su vulnerabilidad: dicho de otra forma, trata de descifrar los criptogramas.

En el análisis para establecer las posibles debilidades de un sistema de cifrado, se han de asumir las denominadas condiciones del peor caso:

1. el criptoanalista tiene acceso completo al algoritmo de encriptación.
2. el criptoanalista tiene una cantidad considerable de texto cifrado.
3. el criptoanalista conoce la pareja de un texto cifrado con su texto en claro.

También se asume generalmente el *Principio de Kerckhoffs*, que establece que la seguridad del cifrado ha de residir exclusivamente en el secreto de la clave, y no en el algoritmo de cifrado como el DES, AES, etc....

Aunque para validar la robustez de un criptosistema normalmente se someten a todas las condiciones del peor caso, existen ataques más específicos, en los que no se cumplen todas estas condiciones. Como son ataques por fuerza bruta o peor aun por diccionario.

Si el atacante conoce el algoritmo de cifrado y sólo tiene acceso al criptograma, se plantea un ataque sólo al criptograma; un caso más favorable para el criptoanalista se produce cuando el ataque cumple todas las condiciones del peor caso; en este caso, el criptoanálisis se denomina de texto en claro conocido. Si además el atacante puede cifrar una cantidad indeterminada de texto en claro al ataque se le denomina de texto en claro escogido; este es el caso habitual de los ataques contra el sistema de verificación de usuarios utilizado por Unix, donde un intruso consigue la tabla de contraseñas (generalmente /etc/passwd) y se limita a realizar cifrados de textos en claro de su elección y a comparar los resultados con las claves cifradas (a este ataque también se le llama de diccionario, debido a que el atacante suele utilizar un fichero 'diccionario' con los textos en claro que va a utilizar). El caso más favorable para un analista se produce cuando puede obtener el texto en claro correspondiente a criptogramas de su elección; en este caso el ataque se denomina de texto cifrado escogido.

Ataques por fuerza bruta.

El ataque por fuerza bruta consiste en procedimiento en el que a partir del conocimiento del algoritmo de cifrado empleado y de un par texto plano/texto cifrado, probando el cifrado (respectivamente, descifrado) de uno de los miembros del par con cada una de las posibles combinaciones de clave, hasta obtener el otro miembro del par. El esfuerzo requerido para que la búsqueda sea exitosa con probabilidad mejor que la par será 2^N y 1 operaciones, donde N es la longitud de la clave (también conocido como el espacio de claves).

Otro factor determinante en el coste de realizar un ataque de fuerza bruta es el juego de caracteres que se pueden utilizar en la clave. Contraseñas que sólo utilicen dígitos numéricos serán más fáciles de descifrar que aquellas que incluyen otros caracteres como letras.

Este ataque es ineficiente por que puede tardar mucho tiempo, años, miles de años de procesamiento cuando la clave es grande, y puede ser rápido si la clave es pequeña... por eso el algoritmo AES implementa como mínimo una llave de 128 bits que son 16 caracteres ASCII.

Ataques por diccionario.

El ataque por diccionario es muy parecido al ataque por fuerza bruta solo que aquí tenemos un conjunto mas pequeños de valores posibles, este tipo de ataque se basa en que los usuarios eligen claves débiles, esto quiere decir que utiliza nombres del amigos, apellidos, mascotas, fechas, etc... que se pueden encontrar en un diccionario con unas 50,000 palabras, mas aparte algunas otras comunes como 123, 123456, etc...

Por ejemplo:

Aaplicaremos este ataque al archivo password de UNIX:

En sistemas UNIX la claves son codificadas con la función "crypt" la cual esta basado con el algoritmo DES con algunas variaciones que produce un resultado un hash de una sola dirección, esto hace que no se pueda revertir.

La función crypt utiliza un valor aleatorio llamado "salt" el cual esta formado por una cadena de dos caracteres [a-z A-Z 0-9 ./]. Este valor aleatorio permite codificar una misma clave de $4096 = 642$ maneras distintas.

Nota.

Los dos primeros caracteres de una clave codificada, son los valores de "salt", el resto hasta un total de 13 caracteres ASCII es la clave codificada según el valor de "salt".

Una vez que sabemos esto nos queda realizar un código en c para implementar un ataque por diccionario.

```
#include <unistd.h>
#include <string.h>
#include <stdio.h>

char *crypt(const char *key, const char *salt);
char * fdicc="dicES.txt";
char * fpass="/etc/passwd";
char salt[3];
char palabra[32]; //palabra del diccionario
char password[128][13]; //128 claves de 13 caracteres
char c;

int main(void)
{ int i=0,k=0,n=0,ok=0;
  FILE * fd,*fp;
  if((fp=fopen(fpass,"r"))!= NULL)
  { //Carga los passwords
    do{ c=fgetc(fp);
```

```

if(c!=':')i++;
else { if(c=='\n'){ n=0; i=0; k++; }
      else if(i==1)password[k][n++]=c;
      }
}while(c!=EOF);

//Proceso de comparar el passwords con crypt(dccc[i])
for(k=k-1; k>=0; k--)
{ ok=0;
  printf("\n[%s]",password[k]);
  salt[0]=password[k][0];
  salt[1]=password[k][1];
  salt[2]='\0';
  for(i=0;i<11;i++)password[k][i]=password[k][i+2];
  password[k][i]='\0';
  printf("[%s][%s]",salt,password[k]);
  if( (fd=fopen(fdicc,"r")) != NULL)
  { do{ if(ok)break;
    c=fgetc(fd);
    if (c=='\n')
    { if(strcmp(password[k],crypt(palabra,salt))==0)
      { ok=1;
        printf("=== %s\n",palabra);
      }
      n=0;
      palabra[n]='\0';
    }
    else palabra[n++]=c;
  }while(c!=EOF);
  fclose (fd);
  if(!ok)printf("....No se encontro\n");
}
}
fclose(fp);
}
return 0;
}

```

Ataques por Análisis de frecuencia

El cálculo de la frecuencia de letras en una lengua es difícil y está sujeto a la interpretación. Se cuenta la frecuencia de las letras de un texto arbitrariamente largo, pero en los resultados influyen varios parámetros:

El estilo narrativo. Si hay muchos verbos en infinitivo, habrá muchas "R".

El vocabulario específico del documento. Si se habla de ríos, habrá muchas "Í"; si uno de los protagonistas se llama Wenceslao, aumentará el número de "W".

La presencia de caracteres no alfabéticos (signos de puntuación, cifras, paréntesis, símbolos matemáticos corrientes...) pueden o no tenerse en cuenta. La coma, punto son por ejemplo más frecuentes que más de la mitad de las letras.

Si estos parámetros tienen un impacto espectacular en los símbolos menos frecuentes, es también sensible incluso para las letras más frecuentes.

Porcentaje de aparición de letras

Existen muchos otros ataques muy bien documentado que se puede encontrar en Internet.

2.3 Funciones hash

Es una función resumen, es un método para generar claves o llaves que representen de manera única a un documento, registro, archivo, etc.

Estos métodos son muy variados, pueden llegar a tomar en cuenta diversos parámetros tales como el nombre de un archivo, su longitud, hora de creación, datos que contenga, etc. aplicándole diversas transformaciones y operaciones matemáticas.

Existen muchos algoritmos para la creación de funciones de resúmenes entre los más comunes son:

- **MD2** (acrónimo inglés de Message-Digest Algorithm 2, Algoritmo de Resumen del Mensaje 2) es una función de hash criptográfica desarrollada por Ronald Rivest en 1989. El algoritmo está optimizado para computadoras de 8 bits. El valor hash de cualquier mensaje se forma haciendo que el mensaje sea múltiplo de la longitud de bloque en el ordenador (128 bits o 16 bytes) y añadiéndole un checksum. Para el cálculo real, se utiliza un bloque auxiliar 48 bytes y una tabla de 256 bytes que contiene dígitos al azar del número pi.
- **MD4** es un algoritmo de resumen del mensaje (el cuarto en la serie) diseñado por profesor Ronald Rivest del MIT. Implementa una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes. La longitud del resumen es de 128 bits. El algoritmo ha influenciado diseños posteriores, tales como el MD5, el SHA o el RIPEMD-160. Ciertas debilidades en MD4 fueron demostradas por Den Boer y Bosselaers en un documento publicado en 1991. Muchos de los diseños posteriores de resumen del mensaje basados en él siguen siendo seguros, en el sentido que no se ha publicado ningún ataque eficaz contra ellos.
- **MD5**. En criptografía, MD5 (acrónimo de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. El código MD5 fue diseñado por Ronald Rivest en 1991. Durante el año 2004 fueron divulgados ciertos defectos de seguridad, lo que hará que en un futuro cercano se cambie de este sistema a otro más seguro.
- **SHA**. La familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos

años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (todos ellos son referidos como SHA-2).

- **RIPEMD-160** (acrónimo de RACE Integrity Primitives Evaluation Message Digest, primitivas de integridad del resumen del mensaje) es un algoritmo del resumen del mensaje de 160 bits (y función criptográfica de hash) desarrollado en Europa por Hans Dobbertin, Antoon Bosselaers y Bart Preneel, y publicados primeramente en 1996. Es una versión mejorada de RIPEMD, que estaba basado sobre los principios del diseño del algoritmo MD4, y es similar en seguridad y funcionamiento al más popular SHA-1.

Ejemplo como hacer un hash.

El algoritmo consiste en tomar un archivo o texto y dividirlo en bloques de 128 bits y realizar una operación bit a bit con un XOR si el bloque es muy pequeño lo repetimos hasta completar los 128 bits de igual forma para el último bloque. El resultado es de 128 bits en hexadecimal.

```
<?php
function fxor($A,$R)
{ for($i=0,$C=""; $i<16; $i++)$C.=chr( ord($A[$i]) ^ ord($R[$i])
);
return $C;
}
function myhash($M)
{ $n=strlen($M); $i=0;
if($n>32)while($n%16)$M[$n++]=$M[$i++]; //completar bits
else while($n<32)$M[$n++]=$M[$i++]; //caracteres 512bits
$R=""; //Resultado
$A=""; //Bloque A
for($i=0; $i<$n; $i+=16)
{ if(!$i){ $R=substr($M,0,16); $i=16; /*Bloque inicial*/ }
$A=substr($M,$i+16,16); //Bloque A
$R=fxor($A,$R); //XOR para los bloques;
}
for($i=0,$C=""; $i<16; $i++)$C.=dechex(ord($R[$i]));
return $C;
}
echo myhash(file_get_contents('http://www.mygnet.com'));
?>
```

Al realizar la prueba con la página web <http://mygnet.com> genera un resumen diferente cada vez que cambia un segundo de la fecha:

Resultados:

```
50e7d6e4e8bef9cf03c89c2a29b2081
6606cbabbd24732cc8f9c8584d325e5
4ecb2c428ea31b59e937c97f48049a1
6f557fa6edb2a13fabbc685fece12fe
```

Nota. Este código es para ejemplificar la construcción de una función hash, pero para que sea correcto debe de pasar por una serie de pruebas y para que no existan colisiones.

2.4 Construcción de protocolos seguros.

Hasta este punto ya tenemos nociones de la criptología tanto históricas como modernas y sabemos lo tipos de ataques que deben soportar los criptosistemas para considerarse seguros, en base a esto hay que proteger los servicios de seguridad que necesitamos para un sistema u organización.

Si yo digo que quiero confidencialidad que vamos a utilizar?

Si envié un mensaje de A a B y quiero que solo B lo descifre?

Recuerda que por naturaleza las redes son inseguras, fueron echas sin pensar en el paradigma de seguridad, si envié un texto en claro, es interceptado y puede ser leído por un tercero o intruso, este puede ser alterado y reenviado con fines particulares del intruso o simplemente puede ver la información que puede utilizar en cualquier momento.

Entonces tenemos que usar la criptografía para la confidencialidad, de hecho para casi todos los servicios de redes vamos utilizar la criptografía donde vamos a combinar diferentes técnicas y algoritmos de cifrado.

2.4.1 Protocolo para la confidencialidad

En particular este caso es el más común con el cual nos vamos enfrentar. Tenemos a A y B que son nodos o entes que quieren comunicarse pero no quieren que los mensajes viajen en claro, por que la información que van a compartir es clasificada como secreta.

Objetivo. Es enviar información de A a B y viceversa donde solo ellos dos puedan saber el mensaje.

Suposiciones.

1. A y B comparten una llave 128 bits que previamente acordaron la cual la vamos a llamar como K.
2. A y B acordaron también el algoritmo a utilizar: AES en operación CBC.
3. A y B cuentan con las condiciones computacionales para el procesamiento de estos algoritmos.
4. Etc...

Protocolo:

A: cifra el Texto en claro con la llave K con AES-CBC.

A: envía el texto cifrado a B.

B: recibe el texto Cifrado.

B: descifra el texto con la llave K con AES-CBC.

Ya tenemos el protocolo de confidencialidad, se hace lo mismo cuando B envía un mensaje cifrado a A.

Veamos si existe escenario de ataque.

Alguien que no sea A o B puede descifrar el mensaje?

No verdad.

Alguien que no sea A o B puede obtener el texto cifrado? Si, pero no le serviría de mucho por que como la información viaja cifrada, no podría leerlo.

Este protocolo cumple con la confidencialidad, pero nótese que aquí existen todas las condiciones, ya que se acordó la llave entre A y B.

Lo único que puede hacer el intruso es recabar todos los mensajes cifrados y almacenarlos para posteriormente hacer criptoanálisis, que pasaría si el algoritmo fuese el cifrado de cesar, o algún otro algoritmo clásico, pues se implementaría un criptoanálisis por frecuencias, verdad...

Todos los algoritmos de cifrado que tenga una llave se pueden atacar por fuerza bruta o por diccionario, esto depende del tamaño de la llave a utilizar y el uso de una llave fuerte es decir utilizar letras, número y caracteres especiales para la conformación de la llave.

2.4.2 Protocolo para la integridad.

Si lo que nos interesa es que nuestros mensajes lleguen íntegros de A a B y viceversa, es decir que los mensajes viajen en texto claro pero no queremos que sean cambiados.

Por ejemplo si un Director manda un mensaje a un Subdirector de una empresa X, dando instrucciones de algo, por que eso suelen hacer lo Directores, que pasaría si un intruso intercepta el mensaje y solo cambia algunas cosas para que la orden del director se diferente.

El ataque aquí es muy sencillo, I que es el intruso, para el mensaje que vienen A que es el director, I entonces los edita para su conveniencia y se lo envía ya modificado a B que es el subdirector. Entonces B lo recibe la orden.

Como evitaríamos este tipo de ataque con la criptografía?

Claro lo que estas pensando eso es, con funciones Hash.

Están seguros que solo con funciones hash?, esta bien hay que hace la prueba.

A: calcula la función Hash del mensaje.
A: envía el mensaje en texto claro pero le anexa el hash del mensaje.
B: recibe el mensaje y el hash que envió A.
B: calcula el hash del mensaje y compara con el que recibió de A, si son iguales quiere decir que no sufrió modificaciones el mensaje, y todos felices.

Vamos a ver si no existe escenario de ataque para este protocolo. Que pasaría si I que es el intruso, obtiene el mensaje y lo modifica, claro ya no va coincidir el mensaje con el hash, verdad.

Pero que pasaría si I, recalcula el hash del mensaje modificado, **Ups**, este si que es un problema, por que cuando llegue el mensaje con su hash a B, va coincidir, verdad!.

Bueno entonces hay que hacer una modificación al protocolo anterior, ya que no requerimos confidencialidad, no vamos a cifrar el mensaje, solo requerimos integridad, entonces que vamos a cifrar?.

Claro que si, el hash.

No hay que olvidar los supuestos como el objetivo son importante para cada protocolo.

Objetivo. Es enviar información de A a B donde se compruebe la integridad del mensaje.

Suposiciones.

1. A y B comparten una llave 128 bits que previamente acordaron la cual la vamos a llamar como K.
2. A y B acordaron también el algoritmo a utilizar: AES en operación CBC
3. A y B acordaron el algoritmo de hash que van utilizar, MD5.
4. A y B cuentan con las condiciones computacionales para el procesamiento de estos algoritmos.
5. Etc...

Protocolo.

A: calcula la función Hash del mensaje.
A: cifra el hash del mensaje con AES-CBC utilizando la llave K.
A: envía el mensaje en texto claro y anexa el cifrado del hash del mensaje.
B: recibe el mensaje en texto claro y el hash cifrado que envió A.
B: descifra el hash del mensaje recibido.
B: calcula el hash del mensaje y lo compara con hash descifrado que recibió de A, si son iguales quiere decir que no sufrió modificaciones el mensaje, y ahora si todos felices.

Aquí ya no hay posibilidad de ataque, por que si I intercepta el mensaje y lo cambia, no sabe la llave que comparte A y B para recalculer el hash.

2.4.3 Protocolo para la Integridad y confidencialidad

Hasta este punto estoy seguro que ustedes ya pueden hacer este protocolo.

Se trata que la información llegue íntegra y que sea confidencial. Bueno este protocolo se resumen al primero, por que ya que solo A y B comparten la misma llave y si uno de ellos envió el mensaje, y no pudo ser alterada por que para editarla I tendría que saber la llave.

Pero si quieren hacer algo mas completo, pues tendríamos que calcular el hash del mensaje y mandarlo junto con el mensaje cifrado todo con K y utilizando un algoritmo de cifrado.

2.4.4 Protocolo para la autenticación mutua.

Este protocolo es para autenticar quien esta mandando el mensaje, si es A es quien dice ser. Los protocolos anteriores todos son de autenticación pero unidireccional, lo que quiere decir que solo se esta autenticando A ya que A envía el mensaje, y al ser descifrado por B, entonces B comprueba que ha sido enviado por A, y que nadie mas que el, por que tiene la llave.

Solo falta que B se autentique. Esto es de la misma manera cuando B envía un mensaje cifrado y A lo descifra, A comprueba que B es el que solo pudo enviar el mensaje por la misma razón anterior. a esa autenticación se le conoce como autenticación mutua.

Si tenemos el siguiente protocolo para autenticación por medio de un nombre de usuario y contraseña.

Seria de la siguiente manera:

A: envía el siguiente mensaje a B; quiero conectarme
 B: responde; quien eres?
 A: dice; soy martin
 B: responde martin, dame tu contraseña?
 A: dice; 123456
 B: Ok, compara con la base de datos y dice Ok; si eres martin, pásale.

A: puede pasar por que ya se autentico.

El primer error de este protocolo de autenticación es que todo viaja en texto claro, y el Intruso la puede obtener, este es el caso del protocolo TELNET, que la autenticación viaja en claro.

Bueno, repensamos un poco este protocolo y le agregamos la criptografía:

E = cifrar
 D = descifrar.

A: envía el mensaje a B pero cifrado; E(quiero conectarme)
 B: responde cifrado también; E(quien eres?)
 A: dice; E(soy martin)
 B: responde; E(martin, dame tu contraseña?)
 A: dice; E(123456)
 B: Ok, compara con la base de datos y dice Ok; E(si eres martin, pásale).
 A: entonces puede pasar.

Aquí hay varios problemas todavía si bien es cierto ya no se envía en claro, pero se sigue enviando la contraseña la contraseña nunca es recomendable que se envíe, mas bien lo que se envía es algo que conoce B y se cifra con la contraseña de tal manera que al recibirlo B lo descifra y compra lo que ya sabe y auténtica al usuario.

Bueno independiente mente de lo anterior.

Hay que buscar un escenario de ataque.

Que pasaría si I que es el intruso, va capturando el texto cifrado que va enviando A a B, de tal manera que depuse I envía el primer mensaje cifrado que capturo de A y se lo envía a B, y B le responde:

B: E(quien eres?)
 I: Segundo texto cifrado
 B: responde; E(martin, dame tu contraseña?)
 I: responde con el tercer texto cifrado
 B: Ok, compara con la base de datos y dice Ok; E(si eres martin, pásale).
 I: entonces I puede entrar.

A este tipo de ataque se le conoce como ataque de replica. Como hacer un protocolo que sea seguro para un ataque de replica.

Si A como B generan números pseudoaleatorios y los utilizan solo una vez por cada envío del mensaje.

El protocolo quedaría de la siguiente manera:

N= Numero pseudoaleatorio único, solo una ves por cada mensaje
 A envía a B: E(quiero conectarme; Na1), B ya no va a recibir ningún mensaje con Na1
 B envía a A: E(quien eres?;Nb1;Na1), B regresa el Na1 y agrega un numero Nb1 de el
 A envía a B: E(soy martin; Na2;Nb1), A compara su Na1 con el que envió y envía Nb1 y Na2
 B envía a A: E(martin, dame tu contraseña?;Nb2;Na2) B compara sus numero Nb1 y envía un Nb2
 A envía a B: E(123456;Na3;Nb2) A compara Na2 y envía un Na3
 B envía a A: E(si eres martin, pásale; Nb3;Na3). Lo mismo....
 A: entonces puede entrar.

Veamos aquí si sigue existiendo el ataque de replicas, Dado que el protocolo exige que por cada envío de mensaje se envíe un numero generado pseudoaleatoriamente, esto con la finalidad de no se puedan replicar los mensajes cifrados por un intruso.

Existe un escenario de ataque, a este protocolo, bueno eso les queda de tarea?

2.4.5 Protocolos para Diffie-Hellman.

Este protocolo es muy útil para el intercambio de claves para criptografía simétrica.

El protocolo Diffie-Hellman (debido a Whitfield Diffie y Martín Hellman) permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo. Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión.

Bibliografía.

<http://es.wikipedia.org/>
<http://serdis.dis.ulpgc.es/>

Espero que este artículo les sea de utilidad o por lo menos sirva de bases para la seguridad a la hora de hacer sistemas...

Boletín Software libre

Lianet Falcón Seijo
 mirtha.seijo@infomed.sld.cu

Este boletín es de libre distribución, todo aquel que quiera colaborar solo tiene que escribirme.



Saludos :-)

En el pasado boletín pudieron leer algunos datos sobre el padre del Software libre, ahora les hablaré sobre Marcelo Tosatti, algo sobre Licencias y podrán conocer las últimas noticias referentes al Free Software.

Lianet

Marcelo Tosatti



Comenzó a trabajar con una computadora cuando apenas tenía 11 años, gracias a su hermano que las armaba para venderlas. Estudió hasta la secundaria básica, pero ya a los doce años conocía de software libre, a los 13 trabajaba para una compañía de su país, y con solo 18 años se convirtió en el

mantenedor del núcleo de Linux en su versión 2.4. en noviembre del año 2001 lanzando el núcleo 2.4.16 el 26 de noviembre.

Marcelo Tosatti nació en el sur de Brasil en Curitiba, Paraná, descubrió su interés por la informática y gracias al método "aprender es compartir y colaborar conocimiento", hoy este joven brasileño, con tan solo 18 años ha sido designado para mantener la rama estable del núcleo de Linux en reemplazo del histórico Alan Cox. Como el resto de los programas de código abierto, Linux es el resultado del esfuerzo colectivo de una legión de programadores que -a través de la Red- piensan y trabajan juntos en el desarrollo del sistema.

Presente en el IV Fórum Software Livre de Porto Alegre, es uno de los más brillantes de los expertos y líderes tecnológicos. Integrante de esa comunidad que en los años sesenta en el Laboratorio de Inteligencia Artificial (Artificial Intelligence Lab) del Massachusetts Institute of Technology (MIT), llamaron hackers La creación tecnológica de los hackers, estos expertos

que llegan a las fronteras de la innovación tecnológica, ha sido decisiva en todo el conjunto de la revolución tecnológica actual.

En una entrevista dice:

"Es quizás el peor trabajo que pueda tenerse", afirma medio en broma. "Pero en realidad es bonito, aunque complejo, pues la comunicación con el resto de los desarrolladores se realiza a través de Internet, de las listas de discusión".

"Desarrollar el software libre hoy es sumamente importante, porque adquirir cualquier software propietario es como comprar un carro al que no se le puede abrir el capó; usted no sabe cómo funciona, cómo está hecho, y eso lo hace una especie de esclavo de quien le vendió el programa. Con el software libre no solo puede utilizar esa tecnología, sino dominarla por completo, saber cómo trabaja, y además modificarla de acuerdo con sus necesidades".

Entrevista A cargo de Amaury E. del Valle

Licencias



Una licencia es aquella autorización formal con carácter contractual que un autor de un software da a un interesado para ejercer "actos de explotación legales". Pueden existir tantas licencias como acuerdos concretos se den entre el autor y el licenciatario. Desde el punto de vista del software libre, existen

distintas variantes del concepto o grupos de licencias:

Las libertades definidas anteriormente están protegidas por licencias de software libre, de las cuales una de las más utilizadas es la Licencia Pública General GNU (GPL). El autor conserva los derechos de autor (copyright), y permite la redistribución y modificación bajo términos diseñados para asegurarse de que todas las versiones modificadas del software permanecen bajo los términos más restrictivos de la propia GNU GPL. Esto hace que no sea imposible crear un producto con partes no licenciadas GPL: el conjunto tiene que ser GPL.

Licencias estilo BSD, llamadas así porque se utilizan en gran cantidad de software distribuido junto a los sistemas operativos BSD. El autor, bajo tales licencias, mantiene la protección de copyright únicamente para la renuncia de garantía y para requerir la adecuada atribución de la autoría en trabajos derivados, pero permite la libre redistribución y modificación, incluso si dichos trabajos tienen propietario. Son muy permisivas, tanto que son fácilmente absorbidas al ser mezcladas con la licencia GNU GPL con quienes son compatibles.

Puede argumentarse que esta licencia asegura "verdadero" software libre, en el sentido que el usuario tiene libertad ilimitada con

respecto al software, y que puede decidir incluso redistribuirlo como no libre. Otras opiniones están orientadas a destacar que este tipo de licencia no contribuye al desarrollo de más software libre.

Licencias estilo MPL y derivadas. Esta licencia es de Software Libre y tiene un gran valor porque fue el instrumento que empleó Netscape Communications Corp. para liberar su Netscape Communicator 4.0 y empezar ese proyecto tan importante para el mundo del Software Libre: Mozilla. Se utilizan en gran cantidad de productos de software libre de uso cotidiano en todo tipo de sistemas operativos. La MPL es Software Libre y promueve eficazmente la colaboración evitando el efecto "viral" de la GPL (si usas código licenciado GPL, tu desarrollo final tiene que estar licenciado GPL). Desde un punto de vista del desarrollador la GPL presenta un inconveniente en este punto, y lamentablemente mucha gente se cierra en banda ante el uso de dicho código. No obstante la MPL no es tan excesivamente permisiva como las licencias tipo BSD. Estas licencias son denominadas de copyleft débil. La NPL (luego la MPL) fue la primera licencia nueva después de muchos años, que se encargaba de algunos puntos que no fueron tenidos en cuenta por las licencias BSD y GNU. En el espectro de las licencias de software libre se la puede considerar adyacente a la licencia estilo BSD, pero perfeccionada.

Hay que hacer constar que el titular de los derechos de autor (copyright) de un software bajo licencia copyleft puede también realizar una versión modificada bajo su copyright original, y venderla bajo cualquier licencia que desee, además de distribuir la versión original como software libre. Esta técnica ha sido usada como un modelo de negocio por una serie de empresas que realizan software libre (por ejemplo MySQL); esta práctica no restringe ninguno de los derechos otorgados a los usuarios de la versión copyleft. También podría retirar todas las licencias de software libre anteriormente otorgadas, pero esto obligaría a una indemnización a los titulares de las licencias en uso. En España, toda obra derivada está tan protegida como una original, siempre que la obra derivada parta de una autorización contractual con el autor. En el caso genérico de que el autor retire las licencias "copyleft", no afectaría de ningún modo a los productos derivados anteriores a esa retirada, ya que no tiene efecto retroactivo. En términos legales, el autor no ha derecho a retirar el permiso de una licencia en vigencia. Si así sucediera, el conflicto entre las partes se resolvería en un pleito convencional. *Más en próximos boletines..*

Noticias

fuelle: www2.noticiasdot.com

Red Hat abre oficinas en Argentina y Brasil
La empresa de software abierto adquirió dos subsidiarias locales de su principal distribuidor.

26 Mayo del 2006



La empresa especializada en software abierto Red Hat anunció la apertura de oficinas en Argentina y Brasil, luego de haber adquirido dos subsidiarias locales de su principal distribuidor.

A partir de la apertura de sus nuevas oficinas regionales -instaladas en San Pablo y en Buenos Aires- Red Hat asegura que *"brindará soporte regional, actividades de capacitación y comerciales, así como también ofertas localizadas"*.

El nuevo puesto de Gerente General en el Cono Sur para Red Hat será para el argentino Julián Somodi, partner y reseller de Red Hat en Sudamérica por más de dos años. Según informó la empresa, Somodi tiene más de 20 años de experiencia en el mercado tecnológico y una amplia trayectoria en la región, ya que se desempeñó en otras compañías del sector como Oracle y Apple Computer.

Aunque hasta ahora no poseía oficinas propias, Red Hat América Latina posee varios clientes en la región como Serpro, Poder Judicial de Perú, Ministerio de Salud de Buenos Aires y Bradesco, entre otros.

Según Red Hat, la expansión de las operaciones directas en la región *"permitirán un mayor desarrollo en las relaciones con los clientes directos y ampliará la fidelización de los partners."*

"Somos un mercado emergente", declaró Somodi, "por lo tanto necesitamos sistemas de bajo costo y de gran potencialidad. Linux es la solución".

La Seguridad Social española se adapta a Linux
El sistema RED de la Seguridad Social, que permite realizar de forma telemática numerosas gestiones como afiliaciones, altas y bajas de trabajadores entre otras, se ha adaptado al sistema Linux, anunció el lunes el Ministerio del Trabajo.

31 mayo del 2006

Agencias - El sistema RED, remisión electrónica de documentos, funciona desde 1995 y lo utilizan todas las empresas con más de 20 empleados, dijo Trabajo en un comunicado.

"La revisión del Sistema RED permite atender a las demandas de una parte de la sociedad española que utiliza el Sistema Operativo Linux", dijo Trabajo.

Esta adaptación pretende avanzar hacia la neutralidad tecnológica de las administraciones públicas, agregó.

La información y software está disponible en www.seg-social.es.

Google apoya a Firefox con más de 80 millones de dólares

En este oleaje de alianzas y fusiones de empresas informáticas para lograr una mayor competitividad en el mercado tecnológico, Google

está apoyando fuertemente el desarrollo del nuevo Firefox 2.0 empleando desarrolladores y destinando personal para colaborar con la Fundación Mozilla. La excelente relación entre ambos significa unos ingresos extra para la Fundación que podrían superar los 80 millones de dólares.

1 junio del 2006



Aparentemente, las especulaciones acerca de que Google estaba fabricando un navegador web no eran ciertas. Al menos no del todo.

El CEO del megabuscar, Eric Schmidt, desmintió la existencia de planes orientados a competir con el Internet Explorer ante un grupo de analistas en Wall Street. "Parece que las personas ya tienen buenos browsers entre los que elegir", dijo y agregó que "no crearemos un navegador sólo por la diversión de hacerlo", dice la agencia Reuters.

Sin embargo, la empresa alienta a sus consumidores a usar una variedad de alternativas al IE, particularmente al gratuito Firefox.

¿Cómo? La página de inicio por defecto de Firefox incluye un cuadro de búsqueda de Google. Al mismo tiempo, el buscador por defecto en la barra de búsqueda de Firefox es Google. Asimismo, Mozilla recibe dinero por cada búsqueda que un usuario de Firefox realice en Google.

En algunos blogs se especula que esos acuerdos y otros le generan ingresos a Mozilla Corporation por u\$s72 millones, aunque desde la empresa lo niegan y dicen que la cifra es mucho menor.

Al mismo tiempo, Google desde hace tiempo emplea a importantes desarrolladores de Mozilla, como a Ben Goodger, una de las claves en la primera versión de Firefox, liberando a la fundación de los costes "laborales" que significa mantener en Mozilla a expertos con una gran valoración en el mercado.

Más allá de las alianzas comerciales, se conoció una novedad bastante reveladora acerca del papel de Google en esta nueva guerra de navegadores.

En diciembre del 2005 Google creó una aplicación exclusiva para Firefox llamada Google Safe Browsing, que no es otra cosa más que una herramienta anti phishing.

Esa herramienta vendrá incorporada con la nueva versión del Firefox, la 2.0, cuya versión final estará disponible a partir del próximo mes de agosto

Firefox obtendría unos ingresos adicionales de 10 millones de dólares por incluir esta herramienta y aumentaría el peso de

Google en el terreno de los servicios y herramientas para usuarios finales, terreno en el que compite abiertamente con las aplicaciones de Microsoft

Un Sistema Operativo basado en Linux y modificado en Argentina vendió 10 mil licencias en India.

"URLI", una distribución GNU/Linux modificada en Argentina y que se presentó en Cebit 2006, vendió 10.000 licencias a una universidad tecnológica de la provincia de Gujarat en India informó el portal mastermagazine.com

6 junio del 2006

El sistema cuenta con lo que posee en general cualquier distribución GNU/Linux de las grandes: una suite de oficina, programas para administración de e-mails, navegador Firefox, mensajeros, codecs, y se puede actualizar el sistema completo a través de Internet.

"Este sistema se vende tanto bajo modalidad OEM a los ensambladores de PCs como al usuario final en su versión retail. Ya hemos vendido en Argentina 3.000 copias. El precio de las licencias en la India varía entre 20 y 40 dólares, es decir, entre 60 y 120 pesos argentinos, mientras que en Argentina las mismas licencias cuestan entre 9 y 45 pesos" declaró Alex Smith, presidente de Internet URL.



Sabías que

El protocolo empleado en la conexión a Internet, PPP(Point to Point Protocol), es un mecanismo que permite utilizar IP y otros protocolos de red a través de una conexión serie, bien sea ésta una conexión directa(utilizando un cable serie entre dos ordenadores) o una conexión realizada empleando módems y líneas telefónicas.

¿Qué es la Inteligencia Artificial?

Inteligencia artificial, término que, en su sentido más amplio, indicaría la capacidad de un artefacto de realizar los mismos tipos de funciones que caracterizan al pensamiento humano. La posibilidad de desarrollar un artefacto así ha despertado la curiosidad del ser humano desde la antigüedad; sin embargo, no fue hasta la segunda mitad del siglo XX, cuando esa posibilidad se materializó en herramientas tangibles.

El término inteligencia artificial (IA) fue acuñado en 1956 por John McCarthy, del Instituto de Tecnología de Massachussets. En ese año se celebró la conferencia de Dartmouth, en Hanover (Estados Unidos), y en ella, McCarthy, Marvin Minsky, Nathaniel Rochester y Claude E. Shannon establecieron las bases de la inteligencia artificial como un campo independiente dentro de la informática

Más adelante seguiremos hablando de este tema...

Edición y Diseño:

Lianet Falcón Seijo

Noticias del mes

Microsoft Anuncia La Disponibilidad De La Beta 2 De Windows Vista, 2007 Microsoft Office System Y Windows Server

Juan Francisco Berrocal
Berrocal239@hotmail.com



Bill Gates ha dado a conocer en el WinHEC 2006 las características de sus tres productos insignia y sus ventajas para empresas y usuarios.

La conferencia anual de ingeniería de hardware de Microsoft, WinHEC, ha sido el escenario elegido por Bill Gates, Presidente y Arquitecto Jefe de Microsoft, para anunciar la disponibilidad inmediata de la beta 2 de Windows Vista, 2007 Microsoft Office system y Windows Server, cuyo nombre en clave es Windows Server "Longhorn". Esta es la primera vez que la compañía presenta, de forma simultánea, las versiones beta de tres de sus productos insignia.

Frente a cerca de 3.500 expertos en hardware, Bill Gates ha demostrado cómo Windows Vista, 2007 Microsoft Office system y Windows Server "Longhorn" fomentarán la innovación y soportarán las novedades en hardware para hacer frente a las necesidades de los usuarios de todo tipo de periféricos informáticos, dispositivos móviles y sistemas de entretenimiento.

Para más información accede a:
<http://www.microsoft.com/spain/>

El Ministro De Cultura De Brasil Defiende La Ética Hacker

Gustavo Alberto Rodriguez
Gustavo@sasoft.com.ar

BARCELONA (EFE).- El ministro de Cultura de Brasil, Gilberto Gil, defendió la cultura 'hacker' en la apertura del Congreso Global de Internet que comenzó en Barcelona y que durante cuatro días analizará las tendencias y los retos del mundo en red.

"Yo, Gilberto Gil, como ministro de Cultura de Brasil y como músico trabajo cada día con el impulso de la ética 'hacker'", sentenció de manera solemne.

Según el ministro, hay que distinguir los "hacker" de los "cracker" -vulgares piratas informáticos, en su opinión- y destacó a los primeros como "militantes de la contracultura que vieron en el ordenador una fantástica herramienta de comunicación".

Gilberto Gil opuso el mundo "hacker" a lo que ha denominado "ortodoxia analógica reaccionaria", un mundo que apuesta -dijo- por el software libre y al cual "Internet le permite crear espacios de igualdad perenne".

Para el ministro brasileño, "los 'hackers' crean, innovan, resuelven problemas y ejercitan la organización de ayuda mutua y voluntaria", lo que, a su juicio, encaja perfectamente con el espíritu fundacional de internet.

Gil, sin embargo, advierte de que "la revolución tecnológica no puede justificarse sólo por sí misma sino que debe reflejarse en el beneficio y bienestar de los pueblos".

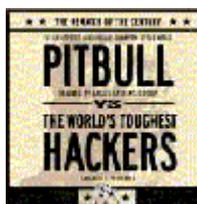
El ministro citó como ejemplo el programa "Una PC para todos", que desarrolla el Gobierno del presidente de Brasil, Luiz Inácio Lula da Silva, para extender el uso de computadoras, que sean accesibles de precio y estén equipadas con software libre.

"Gracias a Internet un indio del Amazonas puede ofrecer sus cestos artesanales a compradores del primer mundo evitando intermediarios y consiguiendo por ello un precio cien veces superior al que tenía antes, al mismo tiempo que el comprador consigue descuentos de decenas de veces", reflexionó Gilberto Gil.

Link corto: <http://www.lanacion.com.ar/810005>

España Registra Un Índice De Piratería Del 46%

Juan Francisco Berrocal
Berrocal239@hotmail.com



Según un estudio realizado, el índice de piratería informática en España sigue subiendo y se sitúa en el 46%, lo que representa unas pérdidas para la industria de 600 millones de euros, un 20% más que el año anterior. España supera en un 10% la media europea, todavía más lejos de lo que estaba en el año 2004.

Según este estudio, se señala el fuerte crecimiento del mercado del PC que no ha podido equipararse al crecimiento de las ventas de licencias de software, lo que ha dejado el índice de piratería en el 46% actual.

La industria del software en España está formada por cerca de 12.000 empresas que dan trabajo a aproximadamente 80.000 personas, además de propiciar otros 300.000 empleos indirectos.

Como conclusión del estudio, si se redujera el índice en 10 puntos de aquí a tres años, se crearían 4.000 empleos más en España.

Detectado Nuevo Virus Ocultado En Archivos Word

Juan Francisco Berrocal
Berrocal239@hotmail.com



Se ha detectado, por varias empresas de seguridad, un nuevo virus que se oculta en documentos de texto de Microsoft Word. Dicho virus aprovecha una vulnerabilidad recién descubierta en Windows XP y Office que podría permitir a un hacker tomar el control de un equipo de forma remota y ejecutar código maligno.

Según declaraciones de la empresa Panda Software, llega oculto en documentos de texto que al ser ejecutados lo liberan. Hasta el momento no se ha descubierto la manera de reenviarse a través de correo electrónico pero al llegar oculto, se ha calificado de altamente peligroso. Panda Software lo ha bautizado con el nombre de 1Table.A

Otras compañías de seguridad, como Symantec y F-Secure, también han detectado este troyano, y lo han bautizado como Trojan.Mdropper.H y Ginwui.A respectivamente.

La empresa Microsoft, implicada como víctima, ha recomentado a los usuarios precaución con los archivos que llegan adjuntos al correo mientras desarrollan un parche para corregir dicho problema.

Apple Vuelve A Descubrir La Piedra De Rosetta

Gustavo Alberto Rodriguez
Gustavo@sasoft.com.ar

El software, bautizado como la célebre pieza de granito, traduce las aplicaciones de Mac para que funcionen con los procesadores de Intel

Hace unos pocos meses Apple sacudió el mercado y, luego de décadas de enfrentamiento, presentó una serie de equipos basados en procesadores Intel, entre los que se cuentan hoy la iMac, las portátiles MacBook Pro y la Mac mini. Detrás de esta innovación surge un conflicto de compatibilidades. Aquel que tenía una Mac con PowerPC y se pasa a una nueva con Intel puede descubrir que algunos de los productos de software que venía utilizando no funcionan con todo su potencial en el nuevo equipo.

Por eso la empresa de la manzanita diseñó *Rosetta*. Es un software de conversión que automáticamente *traduce* una aplicación PowerPC en una Intel, de forma tal que pueda correr nativamente en cualquiera de las dos plataformas. La ventaja de

Rosetta es que, prácticamente, funciona solo. No es necesario configurarlo ni abrirlo.

Simplemente, se hace doble clic sobre la aplicación que se quiere abrir, como siempre. En segundo plano, *Rosetta* hará la traducción de manera dinámica y devolverá la interfaz del software que se abrió con el look & feel exacto con que se lo vio la última vez que se lo haya utilizado en PowerPC.

Las aplicaciones que tienen el sello *Universal* son las que han sido diseñadas para funcionar en ambas plataformas sin inconvenientes. Mac OS X, *iLife 06*, *Safari* y *Mail* pertenecen a este grupo. El problema aparece con los productos llamados *Profesionales*, como *Final Cut Pro*, *Motion*, *Soundtrack Pro*, *DVD Studio Pro*, *Aperture*, *Logic Pro*, *Logic Express*, *Shake* o *Final Cut Express*, que no son naturalmente compatibles con *Rosetta*. En estos casos, los usuarios deberán adquirir la versión *Universal* para poder correr los productos con el mejor nivel a costos relativamente bajos.

En cuanto a las aplicaciones de terceros, la mayoría de los desarrolladores que históricamente han trabajado con Mac ha hecho anuncios respecto de que pronto estarán disponibles sus versiones *Universal*. Por citar sólo dos ejemplos, Adobe presentó un plan de desarrollo que involucra a casi todos sus productos, mientras que Microsoft garantiza que *Office*, *Messenger* y *Remote Desktop Connection* funcionan correctamente en la nueva plataforma.

Walter Duer

Link corto: <http://www.lanacion.com.ar/807489>

Mozilla Firefox Rc 1.0

Christian Palacios Socualaya
Cri1987_9@hotmail.com

Mozilla Firefox RC 1.0 consigue un millón de descargas en tan solo 100 horas. La verdad es que "casi" todo el mundo, que ha probado el navegador lo termina usando. Sus mejoras respecto al IE son más que notables. Versión tras versión han ido corrigiendo fallos y mejorando el navegador, hasta llegar a la versión RC1.0. Según noticias de internet hace poco fueron encontrados 10 errores, de ellos algunos muy graves. Después de leer esta noticia comprobé que en la página de mozilla, ya no estaba disponible para la descarga el Firefox RC1.0. Esperemos que los errores sean corregidos y el navegador siga mejorando día tras día sobre su competencia. Para los que aun no habéis probado el navegador, os invito a que lo probéis descargándolo desde mozilla.org. Seguramente no disponible hasta la corrección de los errores.

Microsoft Anuncia Su Virtual Server 2005 R2

Juan Francisco Berrocal
Berrocal239@hotmail.com

Microsoft anunció su nuevo producto Virtual Server 2005 R2, orientado a la administración de la infraestructura IT. La principal novedad, sin embargo radica en que sobre esta nueva versión del producto podrían correr soluciones Linux.

Cuando se habla de virtualización se hace referencia a tecnología que reduce los costos de la infraestructura IT por medio de la consolidación del servidor, recuperación en caso de desastres, rehospedaje de aplicaciones de legado y evaluación y desarrollo de software. Virtual Server 2005 R2 facilita a las organizaciones que muchas aplicaciones se concentren en un solo servidor ofreciendo grandes niveles de fiabilidad.

Santiago Douton, Gerente de Producto Windows Server System de Microsoft Cono Sur informó sobre los planes de innovación de la compañía. "Luego de varias conversaciones con nuestros clientes detectamos la necesidad de provocar una evolución en el manejo de los sistemas dinámicos. Virtual Server 2005 R2 es la respuesta a esta inquietud".

Sin embargo, el ejecutivo tiene algo más fuerte para declarar sobre esta nueva herramienta: "permite que soluciones Linux puedan correr sobre aplicaciones Microsoft. Este anuncio es un paso importante no sólo para Microsoft sino para toda la industria".

Virtual Server 2005 R2 está disponible mediante una descarga gratuita en el sitio Web de la compañía:

www.microsoft.com/windowsserversystem/virtualserver/

Fuente: <http://www.codejava.org/>

Versión De Was Para Unix/linux

Alfredo De Jesús Gutiérrez Gómez
Neojag@hotmail.com

¡Ya llegó! Por fin está fuera la versión Unix/Linux de Web Application System. Requiere de la presencia del navegador Mozilla y la instalación del módulo Gtk2::MozEmbed. Para ver la lista completa de requerimientos, visitad la documentación en la sección de empaquetado de aplicaciones.

Ya podemos ejecutar nuestras aplicaciones WAS en MS Windows y Unix/Linux sin mayor problema. Esperamos vuestras opiniones.

Sputnik: Una Tecnología De Futuro

Alfredo De Jesús Gutiérrez Gómez
Neojag@hotmail.com

Sputnik es, además de un conocido satélite artificial, nuestra tecnología de gestión de servicios web vía HTTP puro y duro. Al contrario que XML-RPC o SOAP, Sputnik no utiliza ninguna técnica de datos intermedia para realizar la comunicación, sino que esta es producida usando directamente el protocolo estándar de web, permitiendo que cliente y servicio puedan ponerse de acuerdo en el formato, además de realizar la comunicación a mayores velocidades que otros sistemas semejantes.

Tenemos fijado un calendario de nuevas versiones, y os adelantamos las próximas novedades que estamos introduciendo en Sputnik:

- * manejo de datos escalares, listas indexadas y asociativas.
- * manejo de tipos de datos (numeros, fechas, lógicos, etc...).
- * posibilidad de manejar datos globales (compartidos) para el servicio.
- * manejo de servicios web como si fueran clases (atributos y métodos), y generación de objetos basados en servicios.

Ya está disponible para descarga la versión de servidor de Sputnik en PHP para la versión 0.2 del protocolo. Esto aumenta aún más las posibilidades de desarrollo de servicios web con uno de los lenguajes más populares de los últimos años en Internet.

Pasaros por la <http://nettuning.biz/factory/?q=node/22> del proyecto para saber más.

El Pingüino Contrajo Un Virus

Juan Francisco Berrocal
Berrocal239@hotmail.com

Según informes de la empresa especializada en soluciones antivirus Kaspersky, el volumen de amenazas contra Linux se duplicó durante 2005. De todas formas, el volumen de código malicioso para la plataforma de código abierto sigue siendo ínfimo, en comparación con Windows.

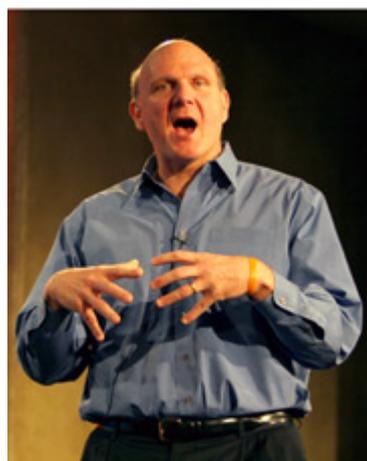
Aunque el número de amenazas contra el sistema operativo de fuente abierta Linux se duplicó en 2005 con respecto al año anterior, según la compañía de seguridad rusa Kaspersky son los usuarios de Mac OS X quienes deberían temer el futuro.

Kaspersky acaba de publicar los resultados del análisis de su base de datos, y afirma que en 2005 encontró 863 códigos maliciosos diseñados para Linux, más del doble que el año anterior, cuando se hallaron unos 422 códigos.

"No es sorprendente, ya que Linux es el sistema operativo más popular del sistema Unix", indicó Konstantin Saprionov, autor del informe y analista de virus de Kaspersky. De todas formas, la cifra sigue siendo ínfima si se la compara contra los más de 11000 códigos maliciosos encontrados para Windows sólo durante la primera mitad de 2005. Es decir, que la plataforma Linux sufre apenas el 4 por ciento de los ataques que sienten los usuarios del sistema operativo de las ventanas.

Microsoft Se Da Cinco Años Para Alcanzar A Google Y Yahoo! En Publicidad 'on Line'

Christian Palacios Socualaya
Cri1987_9@hotmail.com



Steve Ballmer, presidente ejecutivo de Microsoft, sabe que su compañía llega "un poco tarde" al mercado de la publicidad 'on line'.

De hecho, se han marcado un plazo de cinco años para alcanzar a sus principales competidores, Google y Yahoo!. Pero la apuesta es fuerte, puesto que en este ejercicio (que acaba el 30 de junio) Microsoft habrá gastado un 6.200 millones de

dólares para mejorar.

La publicidad 'on line' es un sector lucrativo y en crecimiento liderado actualmente por Google y Yahoo!, que introducen constantes mejoras en sus sistemas. Forrester Research prevé que crezca hasta los 26.000 millones de dólares anuales en 2009 desde los 15.000 que mueve en la actualidad.

Microsoft no quiere quedarse atrás y Ballmer ha comentado que confía en la capacidad de la compañía para desarrollar nuevas tecnologías que les ayuden a alcanzar a los líderes del sector. Por supuesto, no está contento con este retraso, que desde su punto de vista durará unos cinco años.

"No creo que sea una transformación de la noche a la mañana", ha comentado. "Va a tener que ser a largo plazo. Tiene sentido hablar de unos cinco años", ha agregado en unas declaraciones efectuadas en Silicon Valley

Spyxposer Detecta Más De Seis Millones De Spyware Durante 2006

Juan Francisco Berrocal
Berrocal239@hotmail.com



SpyXposer es un potente aplicación gratuita diseñada para la detección de spyware, así como dialers, herramientas de hacking, jokes, riesgos de seguridad o hoaxes. El software espía se ha convertido en una de las principales amenazas de Internet. Se estima que el 90% de los ordenadores están infectados por algún ejemplar de spyware.

La herramienta de análisis online bajo demanda y gratuita SpyXposer ya ha detectado más de 6 millones de ejemplares de spyware durante lo que llevamos de 2006. Este dato pone de manifiesto el peligro que el software espía representa actualmente, y que no solamente pone en peligro la privacidad de los datos de los usuarios, sino que también provoca problemas en los ordenadores en los que se instalan, tales como bloqueos inesperados, ralentizaciones, etc.

Desde hace años Panda Software dedica recursos y personal especializado a la lucha contra esta amenaza de Internet, lo que permite una gran efectividad de todas sus soluciones a la hora de detectar ejemplares de spyware. Para ello, SpyXposer se actualiza diariamente, por lo que siempre se encuentra protegido frente a las aplicaciones espía más recientes.

El spyware es, sin duda, una de las grandes amenazas de los últimos meses. Según la publicación IT Observer1, el 90% de los ordenadores se encuentra infectado por este tipo de código malicioso. La razón para ello es que responde a la nueva motivación económica de los autores de malware, ya puede reportar grandes beneficios, bien mediante la venta de los datos recogidos, o empleándolos para el envío de spam o correo publicitario no deseado.

"Con SpyXposer pretendemos minimizar el impacto que el spyware tiene en los ordenadores de todo el mundo. Se trata de un tipo de código malicioso que, tradicionalmente, no ha inquietado demasiado a los usuarios, pero la realidad es que se ha convertido en una de las principales amenazas de Internet. Pensemos, por ejemplo, en la pérdidas económicas de las empresas debido a mermas de la productividad de sus sistemas informáticos", afirma Luis Corrons, director de PandaLabs.

La herramienta SpyXposer se encuentra disponible en la dirección:

http://www.pandasoftware.es/productos/spyxposer/es/spyxposer_principal.htm

Problemas Con Activex Y IE

Alfredo De Jesús Gutiérrez Gómez
Neojag@hotmail.com

Con la nueva Actualización de windows el IE(Internet Explorer) Ocurre el problema en los comandos y lo cual da problemas en banner hechos en Flash etc El problema es un remarcado o borde que si bien el flash tiene un hipervinculo hay que dar click una vez o mas para activarlo y se le quite el borde....

Hay una solución para código HTML relativamente fácil de resolver. Pero en php-nuke es otra historia debido a los tags que no acepta el phpnuke en bloques, el gran problema de los temas que contiene flash. PDT envío esto no como una noticia si no una forma de que ustedes los que saben de phpnuke, coloquen una solución o por lo menos comenten el tema para los usuarios de phpnuke a ver si entre todo o los que saben coloquen una solución.

Gracias de antemano. (el problema pasa si actualizaste en windows la actualización aparece como opcional aunque los millones de usuarios solo le dan descargar e instalar a todas las actualizaciones de microsoft)

Con la nueva actualización de windows el IE (Internet Explorer) ocurre el problema en los comandos y lo cual da problemas en banner hechos en Flash etc. El problema es un remarcado o borde que si bien el flash tiene un hipervínculo hay que dar click una vez o más para activarlo y se le quite el borde.... Hay una solución para código HTML relativamente fácil de resolver. Pero en php-nuke es otra historia debido a los tags que no acepta el phpnuke en bloques, el gran problema de los temas que contiene flash. PDT envío esto no como una noticia si no una forma de que ustedes los que saben de phpnuke, coloquen una solución o por lo menos comenten el tema para los usuarios de phpnuke a ver si entre todo o los que saben coloquen una solución.

Gracias de antemano. (el problema pasa si actualizaste en windows la actualización aparece como opcional aunque los millones de usuarios solo le dan descargar e instalar a todas las actualizaciones de microsoft)

<http://www.adobe.com/cfusion/webforums/forum/messageview.cfm?catid=194&threadid=1140893&enterthread=y>

Nuevos Factores Para Volar Un Sitio web

Alfredo De Jesús Gutiérrez Gómez
Neojag@hotmail.com

Los buscadores están buscando nuevas herramientas para valorar la calidad de los sitios. De momento no se tiene la certeza de que se esté usando ninguna de ellas, pero aún así, en la blogosfera se están apuntando hacia las siguientes direcciones:

Del.icio.us: Parece ser una fuente de información bastante útil para los buscadores. Tenemos miles de opiniones de usuarios que valoran la calidad del sitio a base de incluirlo en su bookmark, y además organizados mediante tags, con lo cual la clasificación de información se hace realmente ágil.

Google analytics: Un sistema de estadísticas totalmente gratis que proporciona información a los dueños del sitio de las visitas

que reciben, y... a Google también

Google Bookmarks: Lo mismo que del.icio.us pero de la propiedad de Google. Del.icio.us fue comprado por Yahoo! uno de los buscadores que más parecen adelantar en la búsqueda de nuevos métodos de filtraje del spam.

Todos éstos, son recursos que se están vislumbrando como posibles herramientas a manos de los buscadores para mejorar su calidad. Iremos viendo como evoluciona el tema.

Fuente: <http://www.error500.net/futuro-posicionamiento-buscadores>

Secuestro De Documentos

Alfredo De Jesús Gutiérrez Gómez
Neojag@hotmail.com

En este mundo se ve de todo, hoy me acabo de topar con la noticia de que ha salido un nuevo virus (no, ésta no es la noticia que me ha sorprendido) lo que me ha sorprendido es el modus operandi de este virus. El simpático programita te secuestra un documento encriptándolo y luego te pide 300 dólares para devolvértelo. El nombre del virus es Troj/Zippo-A o CryZip y en inglés se conoce como Ransomware.

Hasta el momento, la única vía de contagio de este virus es a través de algunas páginas web, no mediante el correo, la cual cosa ha evitado que se haya extendido a nivel mundial. El mensaje que dejan en el PC de la víctima es el siguiente:

su ordenador ha capturado nuestro software mientras navegaba en una página con contenido pornográfico ilegal, todos sus documentos, archivos de texto, base de datos han sido archivados con una contraseña. No puede descubrir la contraseña para sus archivos –su longitud tiene más de 10 símbolos lo que hace imposible ser descubierta por programas especializados (buscando contraseñas con todas las combinaciones posibles). No busque un programa que ha encriptado sus documentos. Sencillamente ya no existe en su disco duro. Si realmente le interesan sus documentos puede pagar 300 dólares. Informando a la policía sobre un caso no le ayudará. Ellos no conocen la contraseña. Informando sobre nuestra cuenta e-gold tampoco le ayudará a recuperar su información. Hay una sola manera de recuperarlos.

Tal como afirma Annie Gay, Directora General de Sophos Europa del Sur, estamos en una nueva era, ahora los virus ya no son un mero divertimento de adolescentes, sino recursos destinados a ganar dinero.

Fuente:

http://www.libertaddigital.com/noticias/noticia_1276277300.html

Apollo: El Futuro De Flash

Gustavo Alberto Rodriguez
Gustavo@sasoft.com.ar

Adobe está rediseñando el entorno flash para independizarlo de los navegadores web

La empresa Adobe anunció que se encuentra trabajando activamente en una ampliación de la plataforma Flash, un entorno originalmente desarrollado por Macromedia. Uno de los principales objetivos de la compañía será independizar al entorno Flash de los navegadores web, e integrarlo con el lenguaje html y con el formato PDF.

Según un informe especial del sitio news.com, la nueva plataforma –que posee el nombre en clave de Apollo– permitirá superar algunas de las limitaciones que posee Flash en la actualidad. De acuerdo con Adobe, el nuevo software estará disponible para su descarga a comienzos del año próximo.

El desarrollo de Apollo se produce en un contexto de febril competencia entre las grandes empresas por suministrar herramientas y nuevas aplicaciones destinadas a ser el soporte de una nueva generación de aplicaciones web. Este tipo de desarrollos está vinculado con interfaces altamente interactivas y flexibles, que permitirán aprovechar al máximo las conexiones permanentes a Internet. Según los analistas, el objetivo de las compañías es reducir las diferencias entre los sitios web, las aplicaciones y el contenido multimedia.

De acuerdo con Adobe, Apollo está dirigido a brindar a los desarrolladores nuevas formas de crear aplicaciones que puedan correr animaciones flash, y que a la vez que soporten HTML y archivos PDF. De esta manera, se seguirá priorizando a la web, pero se dará espacio a aplicaciones que no pueden ser incluidas en el formato actual de Flash.

Por ejemplo, Apollo podrá correr aplicaciones web que seguirán funcionando aunque el usuario se desconecte de Internet. En el caso de volver a conectarse a la red, la aplicación actualizará la información que sea necesaria.

Según Adobe, Apollo se comportará como una aplicación de escritorio ordinaria, es decir como cualquier programa instalado en la PC.

Según Adobe, las primeras versiones de Apollo destinadas a los desarrolladores estarán disponibles antes de fin de año. De todas maneras, los programadores podrán escribir aplicaciones para Apollo mediante las herramientas actuales de la compañía.

Por otro lado, Adobe anunció que profundizará su relación con los lenguajes de "scripting". Así, la próxima versión del reproductor de Flash –la número 9– ha sido reescrita para poder correr secuencias de comando hasta 10 veces más rápido. Cabe recordar que recientemente, Adobe se unió al consorcio Open Ajax, un proyecto que reúne varias empresas interesadas en crear desarrollos AJAX.

Como era de preverse, el principal contrincante de la nueva estrategia de Adobe será Microsoft, que también se encuentra desarrollando plataformas que podrán correrse desde navegadores alternativos y desde distintos sistemas operativos.

Original en:

<http://www.tectimes.com/secciones/notas.asp?codnota=18812>

Google Asegura Que Internet Explorer 7 Limita Las Opciones De Búsqueda

Christian Palacios Socualaya
Cri1987_9@hotmail.com

Google afirma que Internet Explorer 7, la última versión del conocido navegador de Microsoft, limita las opciones de búsqueda al establecer por defecto la tecnología de MSN Search en su nueva ventana de búsquedas integrada, similar a las que ya existen en Firefox u Opera.

Sin embargo, la compañía de Bill Gates ha dicho en un comunicado que Internet Explorer 7 permitirá a los usuarios "escoger el motor de búsqueda que prefieran utilizar", sea Google, Yahoo! o MSN Search.

La nueva versión del Explorer, según Google, reenvía de forma automática a los usuarios a MSN tras una búsqueda, lo que "coloca a Microsoft en posición de recoger injustamente tráfico e ingresos publicitarios", perjudicando a los rivales de la compañía.

Google ya ha expresado su preocupación por este hecho ante el departamento de Justicia estadounidense y la Comisión Europea, pues considera que podría afectar al mercado de las búsquedas en Internet y favorecer una situación de monopolio.

Denegación De Servicio En Sctp-netfilter Del Núcleo Linux

Christian Palacios Socualaya
Cri1987_9@hotmail.com

Denegación de servicio en SCTP-Netfilter del núcleo Linux

Patrick McHardy ha informado, a través de las listas de distribución dedicadas al anuncio de nuevas versiones del núcleo Linux, la disponibilidad de una nueva versión en la rama 2.6

Esta nueva versión, numerada como 2.6.16.13, ve la luz a consecuencia de la detección de un problema de seguridad diagnosticado en versiones anteriores de la rama, problema que podría facilitar enormemente la conducción de ataques de denegación de servicio sobre las máquinas con núcleos vulnerables.

La falla está causada por un error de diseño en el código de SCTP-netfilter, que en versiones sin actualizar no garantiza que

no se produzcan bucles infinitos que tras algunos ciclos pueden llegar a extenuar los recursos disponibles, anulando la capacidad de la máquina.

El parche no es complejo, con un total de 3 ficheros cambiados (incluyendo el makefile) y un total de 15 inserciones y 9 sustracciones en el diff correspondiente. Sin contar el makefile, restan por tanto 14 inserciones (7 por fuente) y 8 sustracciones (4 por fuente) que hay que aplicar en el código fuente de `ip_contrack_proto_sctp.c`, ubicado en `net/ipv4/netfilter/` y en `net/netfilter/`

Sin tener en cuenta las adiciones en el código relativas a comentarios, la esencia del parche consiste en la agregación de una segunda condición de contorno en la que se verifican además los tamaños de las porciones de los fragmentos gestionados a través del protocolo SCTP (Stream Control Transmission Protocol), de modo que se garantice un progreso adecuado y completo para cada particularización inducida por el bucle `for_each_sctp_chunk()`. SCTP es un protocolo en la capa de transporte que facilita el transporte de señales PSTN (Public Switched Telephone Network) sobre redes IP, con un diseño orientado a la seguridad, ya que es un protocolo diseñado específicamente para evitar no sólo las congestiones naturales, sino para proporcionar resistencia a los ataques de inundación (flooding) y de enmascaramiento (maskerading).

Habida cuenta de que este tipo de denegaciones de servicio son factibles no sólo local sino remotamente, el carácter de criticidad asignable al fallo es de moderadamente crítico. Desde estas líneas realizamos un llamamiento a los administradores para que procedan a actualizar tan pronto les sea posible.

Más Información:

Parche 2.6.16.13

<http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.16.13.bz2>

Cambios en 2.6.16.13

<http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.13>

Sun Facilita El Licenciamiento De Java

Gustavo Alberto Rodriguez

Gustavo@sasoft.com.ar

La empresa Sun anunció un plan para reducir las trabas de licenciamiento de su lenguaje Java. La iniciativa se dirige especialmente a los sistemas operativos de código abierto, como Linux, FreeBSD y OpenSolaris. De esta manera, este tipo de plataformas podrán contar con el Java Runtime Environment de Sun (necesario para que Java pueda correr en los equipos), sin ningún tipo de restricciones de licenciamiento.

Según el sitio Beta News, los desarrolladoras han solicitado

insistentemente a Sun que abra el código de Java, con lo que se lograría un mayor avance de la plataforma. A pesar de que la empresa se resiste a tomar esta medida, ha dado pasos concretos para facilitar el acceso a varias partes de su código.

Además de abrir Java en términos de licenciamiento, se espera que Sun haga un anuncio relacionado con su Java Platform Enterprise Edition 5. Se prevé que Sun ofrecerá un kit de desarrollo para facilitar la programación de Java para servidores. Empresas como BEA Systems, Oracle, JBoss y SAP afirman que ya están desarrollando software con el SDK de Java, y que tendrían productos listos para lanzar al mercado en unos 18 meses.

Original en :

<http://www.tectimes.com/secciones/notas.asp?codnota=18800>

Latinux, Nuevo Consorcio Para Apoyar El Software Libre

Gustavo Alberto Rodriguez

Gustavo@sasoft.com.ar

Seis empresas de Brasil, Venezuela, Puerto Rico y los Estados Unidos firmaron un acuerdo de cooperación para el desarrollo de Software Libre

La iniciativa lleva el nombre de "Latinux" y fue presentada durante el '7° Foro Internacional de Software Libre', celebrado en Porto Alegre desde el 19 hasta el 22 de abril pasados.

Tal como publicó el sitio CDTinternet.net, participan en 'Latinux' las compañías brasileñas Propus Informática Ltda. y Solis Cooperativa de Soluções Livres; las venezolanas Instituto Superior de Estudios e Investigaciones Tecnológicas (ISEIT) y Corvus Latinoamerica C.A.; la puertorriqueña RedBoricua.com Inc.; y la estadounidense Alacos. Estas compañías van a concentrar los servicios de soporte, mantenimiento e instalación de soluciones empresariales basadas en Software Libre, en toda América Latina.

De acuerdo con los responsables del consorcio, las empresas participantes en el proyecto van a compartir conocimiento, intercambiar experiencias, promover el Software Libre y cooperar en el trabajo de las comunidades organizadas en torno a dicho software. Otras compañías de Argentina, Perú y Chile también mostraron interés en sumarse al proyecto.

Entre las posibilidades de trabajo que se abren a partir de 'Latinux' están cubrir la demanda no satisfecha de organizaciones, empresas y gobiernos en relación al desarrollo de Software Libre y el aprovechamiento de productos y servicios que tengan éxito en un determinado sitio dentro del área de atención del consorcio.

Nota original en:

www.tectimes.com/secciones/notas.asp?codnota=18790

La Onu Recomienda Uso Del Software Libre

Alfredo De Jesús Gutiérrez Gómez
Neojag@hotmail.com

El organismo considera que las plataformas abiertas propician el desarrollo de los países miembros y recomienda la utilización y el fomento del 'software' libre tanto en el seno de la organización como entre los países miembros. Así lo afirmó el inspector de Naciones Unidas Dominique Ouredrago, durante en la clausura de la II Conferencia Internacional de Software Libre celebrada en Málaga...

Según la Agencia EFE, Ouredrago indicó en dos informes que la ONU considera que el 'software' libre es el vehículo "más adecuado" para el desarrollo de los países miembros, especialmente en materia de salud, educación y comercio internacional.

Los participantes de este encuentro, que reunió a 6.500 personas de 170 países diferentes, coincidieron en que es necesario "un esfuerzo" para acercar el software libre a los usuarios y "entregarles" nuevas funcionalidades.

Dentro de la conferencia se presentaron productos como USEBIX, creado por Iniciativa Focus e Hispalinux, asociación española de usuarios del 'software' libre, consistente en un sistema operativo completo, instalado en una memoria USB.

En la misma línea, la iniciativa 'Guadalinux online' ofrece la tecnología necesaria para que los ciudadanos puedan acceder al sistema Guadalinux V3 a través de internet sin necesidad de cambiar la configuración de su computadora.

Google Pone Fin Al Uso De La Palabra "Linux" Por Parte De Microsoft

Alfredo De Jesús Gutiérrez Gómez
Neojag@hotmail.com

Luego de las diversas denuncias y altruista acción del abogado José María Lancho y la Asociación Linux Español, Google decide poner fin a la abusiva campaña Adwords iniciada este año por Microsoft. Hasta hace horas, al buscar la palabra "Linux" en la versión española del motor de búsquedas Google, el usuario se encontraba con un aviso de Microsoft que enlazaba a una engañosa comparación entre los sistemas operativos Linux y Windows. De esta manera la empresa Microsoft perpetraba impunemente un acto de competencia desleal y publicidad engañosa al que felizmente Google ha decidido dar fin. Damos las gracias al equipo de Google, a José María Lancho de la Asociación Legalventure y a la Asociación Linux Español por ayudarnos a proteger y defender de esta manera el software libre en España .

Revelan Huecos En El Corazón De La Red

Gustavo Alberto Rodríguez
Gustavo@sasoft.com.ar

Simple ataques permitirían a delincuentes cibernéticos, o hackers , tomar control de más de un tercio de los sitios de internet, asegura una investigación recientemente publicada.

El hallazgo surge de un trabajo realizado a partir del análisis de cómo funciona el sistema de direccionamiento de la red de redes.

Los científicos también señalan que si estos simples ataques son combinados con los llamados bloqueos de servicio (denial-of-service attacks), el 85% de la red se revela vulnerable.

La investigación recomienda grandes cambios a la forma en como se enrutan actualmente las páginas de internet si se quiere reducir drásticamente la debilidad del sistema en su propio centro neurálgico.

Tomando control de un sitio

Cuando se visita un sitio de internet, la computadora pregunta a uno de los directorios de la red (servidores de dominio) dónde está físicamente almacenada la página.

Los profesores Emin Gun Sirer y Venugopalan Ramasubramanian del Departamento de Ciencias de la Computación de la Universidad Cornell hallaron que una búsqueda típica involucra, en promedio, a 46 computadoras que contienen diferente información sobre los componentes de cualquier dirección particular.

Esta cadena de dependencias entre las computadoras que enrutan las diferentes partes de una dirección web crea toda clase de vulnerabilidades, que cualquier pirata informático puede explotar fácilmente, señalan los científicos.

El profesor Sirer explica que "el crecimiento de internet ha causado que emerjan estas dependencias. En vez de tener que penetrar un servidor específico, un hacker sólo necesita tomar control de una máquina en varias docenas".

"El actual sistema de dominios (dirección de un sitio web) ha sido increíblemente exitoso hasta ahora, pero está comenzando a mostrar su edad".

"Necesitamos repensar toda la infraestructura de direccionamiento de internet", asegura el científico.

Mark Ward
BBC Tecnología

Link corto: <http://www.lanacion.com.ar/801801>

Unidos Por La Virtualización

Gustavo Alberto Rodriguez
Gustavo@sasoft.com.ar

Más de 20 empresas proveedoras de hardware, software y servicios informáticos unieron sus fuerzas para crear desarrollos vinculados con la virtualización. La nueva Alianza es una iniciativa de la empresa VMware, e incluye a jugadores clave como IBM, HP y Sun Microsystems.

El proyecto, llamado Virtual Desktop Infrastructure Alliance, apunta a consolidar la virtualización de escritorios y a resolver cuestiones vinculadas con la seguridad, privacidad y estandarización de esta tecnología en ascenso.

De acuerdo con Jerry Chen, Director del área de desktops corporativos de VMware, "el outsourcing y el teletrabajo plantean creciente problemas de seguridad, privacidad, y eficacia". Según Chen, uno de los problemas es que los usuarios corporativos se conectan a la red desde locaciones poco seguras. De esta manera, la implementación de software de escritorios virtuales podría ser una solución viable al problema de seguridad, y además podría resolver otras cuestiones relacionadas con la fiabilidad de los sistemas.

Por ejemplo, los administradores de IT pueden alojar y administrar PCs virtuales en sus data centers, y de esta manera están en condiciones de ofrecer las mismas herramientas que tendría el usuario si estuviera físicamente en el lugar.

Según el sitio Internet News, el analista de IDC, Al Gilles, sostiene que los temas de seguridad y eficacia implicados en el desarrollo de máquinas virtuales hacen prever que existe un gran mercado potencial para este tipo de tecnología.

La empresa VMware anunció que trabajará con cada miembro de la alianza para crear, testear, e integrar desarrollos conjuntos basados en la infraestructura de VMware y en el producto o hardware de cada empresa asociada al proyecto.

Algunas de las otras empresas que suscriben el emprendimiento son: Altiris, Appstream, Ardenice, ATOS Origin, Check Point Software Technologies, Citrix, ClearCube Technology, Devon IT, Dunes Technologies, Fujitsu-Siemens, LeoStream, NComputing, NEC, Platform Computing, Propero, Provision Networks, Route1, Softricity, Wyse Technology y Zeus Technology.

El software de estaciones de trabajo de VMware consiste de una suite de máquinas virtuales destinadas a las plataformas compatibles con Intel x86. El sistema de VMware permite la creación y ejecución de múltiples computadoras virtuales en forma simultánea. Cada una de estas máquinas puede ejecutar su propio sistema operativo, como Windows, Linux u otros.

<http://www.tectimes.com/secciones/notas.asp?codnota=18766>

Google Se Juega Por Firefox

Gustavo Alberto Rodriguez
Gustavo@sasoft.com.ar

La empresa Google decidió renovar su apoyo al navegador Google al realizar varias acciones de marketing. La más importante fue la publicación de un anuncio en su página principal, con el objeto de promocionar la versión de Firefox que incorpora la "Google Toolbar".

Aunque Google no acostumbra poner avisos en su página principal, ocasionalmente la compañía promociona productos propios que están combinados con los de otras empresas. Algunos ejemplos de esto son Google Pack, que integra software de varias firmas, y Google Video, que posee contenidos provenientes de la NBA y de CBS. Se espera que las acciones de promoción tengan un impacto significativo en el aumento de porción de mercado de Firefox, que ya supera el 10% del total.

Según una vocera de Google, la presencia de la publicidad de Firefox es una extensión de la promoción del navegador a través del sistema AdSense, que comenzó el año pasado. A través de este programa, Google paga un dólar a sus afiliados por cada copia de Firefox con Google Bar que es descargada. De acuerdo con la compañía "Google está promocionando Firefox con Google Toolbar por que la posibilidad de navegación con pestañas y el recorrido más seguro de la web le brindan a nuestros usuarios una mejor experiencia de búsqueda".

La publicidad de Firefox, que sólo puede ser vista por los usuarios de Explorer en determinadas regiones- hace alusión a una de las principales ventajas del navegador libre: la seguridad. El texto completo del aviso dice "Firefox con Google Toolbar: navegación con pestañas, surfear la web de manera más segura".

En realidad, la estrategia de apoyo a Firefox por parte de Google enmascara algo mayor: la guerra con Microsoft por la hegemonía en el terreno de los navegadores y de la búsqueda online.

Recientemente, Google ha hecho oír sus quejas a distintos organismos reguladores de Europa y Estados Unidos con respecto a la nueva barra de búsqueda de Explorer 7. Para Google, el hecho de que la barra de Explorer tenga por motor predeterminado a Windows Live Search resulta abusivo y que resulta un abuso de posición dominante.

Por su parte, Microsoft alega que la acusación de Google no tiene fundamento y que los usuarios podrán fácilmente cambiar las preferencias del nuevo Explorer, por si desean utilizar otro motor de búsqueda.

<http://www.tectimes.com/Secciones/notas.asp?codNota=18780>

Manuales en el mes

Abap

Definición e impresión de códigos de barra desde sapscrip

Teknoda
sapping@teknoda.com

Tamaño: 143 KB
Manual de 11 páginas en formato pdf.
<http://www.mygnet.com/pages/down.php?man=852>

Lenguaje C

Manual de c (actualizacion)

Joseph
elprogramador83@hotmail.com

Tamaño: 1 MB
Bueno solo es la actualización del manual anterior
<http://www.mygnet.com/pages/down.php?man=866>

Delphi

Empezamos a programar usando

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 129 KB
Se utilizan mas afondo los componentes de delphi
<http://www.mygnet.com/pages/down.php?man=769>

Objet pascal

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 138 KB
Es la programación orientada a objeto en pascal utilizando a delphi, muy explicado
<http://www.mygnet.com/pages/down.php?man=766>

Introducción a delphi

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 346 KB
Detalla los componentes de la ventana en delphi
<http://www.mygnet.com/pages/down.php?man=765>

Excepciones

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 36 KB
Se describe que es una excepción en delphi y como se debe manejar y en que lugar manejarla
<http://www.mygnet.com/pages/down.php?man=771>

Generación de menús y trabajo sin formularios

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 176 KB
Nos adentramos mas afondo para la creación de aplicaciones
<http://www.mygnet.com/pages/down.php?man=770>

Manejo de base datos

Principales controles dirigidos a datos

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 170 KB
Se sigue avanzando en el margen de base de datos
<http://www.mygnet.com/pages/down.php?man=774>

Funcionamiento de tablas planas (II)

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 86 KB
Se muestra un enfoque mas afondo de las bd
<http://www.mygnet.com/pages/down.php?man=773>

Funcionamiento de tablas planas (I)

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 138 KB
Nos adentramos al camino de base de datos
<http://www.mygnet.com/pages/down.php?man=772>

Punteros

Punteros y estructuras en objetpascal

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 73 KB
Se avanza de nivel con el manejo de estructuras se va un poco mas complicado.
<http://www.mygnet.com/pages/down.php?man=767>

Manipulación objetos

Principales controles dirigidos a datos

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 427 KB

Ahora empezamos a crear nuestros propios componentes
<http://www.mygnet.com/pages/down.php?man=775>

Formularios y componentes en delphi

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 159 KB

Muestra el manejo y uso de los componentes de delphi
<http://www.mygnet.com/pages/down.php?man=768>

Diseño gráficos

Corel draw 12

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 884 KB

Lo mejor para ustedes
<http://www.mygnet.com/pages/down.php?man=786>

Modo gráfico

Manual de corel draw 7

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 148 KB

Manual de corel draw 7
<http://www.mygnet.com/pages/down.php?man=783>

Graficación

Manual de corel 10

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 467 KB

Aquí esta todas las herramientas
<http://www.mygnet.com/pages/down.php?man=784>

Diseño web

Dreanweaver

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 1 MB

Todo lo básico

<http://www.mygnet.com/pages/down.php?man=785>

Datos externos

Manual de lenguaje web desde 0

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 38 KB

Manual de lenguaje web desde 0
<http://www.mygnet.com/pages/down.php?man=790>

Flash

Botones con estilos

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 6 KB

Flash

<http://www.mygnet.com/pages/down.php?man=788>

Fox pro

Funciones fox pro

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 1,000 KB

Aquí esta todas las funciones

<http://www.mygnet.com/pages/down.php?man=779>

Código de barras

Luis Martínez
gustavo@sasoft.com.ar

Tamaño: 79 KB

Manual de 10 páginas en formato pdf, sobre códigos de barra en vfp. Publicado por foxpress. el original está en
<http://www.fpress.com/revista/num9811/nov98.htm>
<http://www.mygnet.com/pages/down.php?man=850>

Hardware

Estructura del disco duro

Jorge Alberto Portillo
jorge_steelrock@hotmail.com

Tamaño: 379 KB

Estructura del disco, particiones, tipos de particiones, como particionar un disco a fat con fdisk con win98.

<http://www.mygnet.com/pages/down.php?man=804>

Multimedia

Guía técnica de digitalización

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 220 KB

Muestra como debe de ser una correcta digitalización

<http://www.mygnet.com/pages/down.php?man=778>

Internet

Firefoxinstalacion

Palacios Socualaya Christian

cri1987_9@hotmail.com

Tamaño: 219 KB

Manual de instalación

<http://www.mygnet.com/pages/down.php?man=793>

J2se

Manipulación objetos

Herencia. poli y clases es und *.doc

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 7 KB

Es un *.doc que explica mas afondo los conceptos claves de la poo

<http://www.mygnet.com/pages/down.php?man=822>

Polimorfismo, herencia y clases

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 7 KB

Manual básico de orientación a objetos

<http://www.mygnet.com/pages/down.php?man=815>

Capitulo 2b de java

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 263 KB

Modelo de objetos en java

<http://www.mygnet.com/pages/down.php?man=807>

Capitulo 2a de java

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 179 KB

Introducción al modelado orientado a objetos

<http://www.mygnet.com/pages/down.php?man=806>

Datos externos

Capitulo 1 de java

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 176 KB

Resaltar la importancia del diseño

<http://www.mygnet.com/pages/down.php?man=805>

Java

Introducción al javabuilder

David Ordinola

davidordinola@yahoo.es

Tamaño: 1 MB

Para los amantes del java, un tremendo manual completísimo, y si desarrollas en plataforma jbuilder mejor, pero eso no es lo importante

<http://www.mygnet.com/pages/down.php?man=824>

Introducción al java

David Ordinola

davidordinola@yahoo.es

Tamaño: 604 KB

Un curso completo del lenguaje java, desde lo simple hasta lo complejo, para principiantes y avanzados. gocenlo

<http://www.mygnet.com/pages/down.php?man=823>

Manipulación objetos

Manual de dio sun

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 133 KB

Manual directo de sun con la colaboración de: Juan Antonio Palos (en la traducción)

<http://www.mygnet.com/pages/down.php?man=860>

Java 3

Alfredo De Jesús Gutiérrez Gómez

neojag@hotmail.com

Tamaño: 122 KB

Ejemplo puro de applets

<http://www.mygnet.com/pages/down.php?man=859>

Java 1

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Tamaño: 35 KB
 Manual con ejemplo de applets
<http://www.mygnet.com/pages/down.php?man=858>

Jsp

Creando webservices en java

David Ordinola
davidordinola@yahoo.es

Tamaño: 1 MB
 Para los amantes de la web o los que aun no saben que es un webservice, como funciona o como sea hace, un súper manual y aprendan todo. esta en lenguaje java
<http://www.mygnet.com/pages/down.php?man=825>

.net

Crear un webservice en java e invocarlo desde vs.net

David Ordinola
davidordinola@yahoo.es

Tamaño: 483 KB
 Rapido ejemplo de como combinar dos tecnologias sin ningun problema, creando un webservice en java publicarlo en la web, y usarlo para desarrollar en .net y tambien puede ser al reves ... eso es tarea para ustedes ja :)
<http://www.mygnet.com/pages/down.php?man=826>

Linux

Instalar driver nvidia en linux

Jorge Alberto Portillo
jorge_steelrock@hotmail.com

Tamaño: 38 KB
 Es un muy buen manual espero y les sirva de mucho, igual espero sus comentarios, preguntas y sugerencias debido a q de los errores aprendemos!!
<http://www.mygnet.com/pages/down.php?man=803>

Linux

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 485 KB
 Linux todo
<http://www.mygnet.com/pages/down.php?man=787>

Navegadores

Gateway paso a paso.

Fredy Ramirez Porfirio
hosh.frp@gmail.com

Tamaño: 91 KB
 Es te tutorial explica paso a paso como configurar un gateway en linux.
<http://www.mygnet.com/pages/down.php?man=870>

Mysql

Como instalar la replica de la base de datos en mysql

Fredy Ramirez Porfirio
hosh.frp@gmail.com

Tamaño: 79 KB
 Este manual muestra como crear un servidor de replicas para una base de datos en my sql, utilizandi window xp sp2 como plataforma.
<http://www.mygnet.com/pages/down.php?man=861>

Varios

Autocad

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 1 MB
 Autocad
<http://www.mygnet.com/pages/down.php?man=796>

Tecnología ajax

David Ordinola
davidordinola@yahoo.es

Tamaño: 179 KB
 Un pequeño articulo sobre que e en realidad y como funciona esta nueva combinación de tecnologías llamada ajax
<http://www.mygnet.com/pages/down.php?man=856>

La tecnología rfid

Aida Centre
info@aidacentre.com

Tamaño: 2 MB
 Completo informe sobe esta tecnología, en 43 páginas de formato pdf, publicado por la generalitat de catalunya cidem.
<http://www.mygnet.com/pages/down.php?man=855>

Preguntas frecuentes sobre el código de barras

Azalea Software, Inc.
salesinfo@azalea.com

Tamaño: 84 KB
 Cuatro páginas en pdf
<http://www.mygnet.com/pages/down.php?man=854>

Como obtener un código de barras

Gustavo Alberto Rodriguez
gustavo@sasoft.com.ar

Tamaño: 2 MB
 Manual en formato pdf sobre el ean en paraguay, pero contiene información útil sobre los códigos de barras en general.
<http://www.mygnet.com/pages/down.php?man=853>

Recomendaciones sobre codificación

Gustavo Alberto Rodriguez
gustavo@sasoft.com.ar

Tamaño: 717 KB
 Lacónico y visual manual en 20 páginas de formato pdf, sobre la colocación de códigos de barra. Autor anonomo.
<http://www.mygnet.com/pages/down.php?man=851>

Envases y embalajes - códigos de barra

Yanina María
yaninamaria20@hotmail.com

Tamaño: 129 KB
 Manual de 11 páginas en formato pdf, sobre códigos de barra publicado en monografías
<http://www.mygnet.com/pages/down.php?man=849>

Identificación ean/ucc

Ean Argentina
info@codigo.org.ar

Tamaño: 387 KB
 Identificación ean/ucc para unidades de consumo masivo y unidades logísticas. considerando el gran crecimiento de las herramientas informáticas en procesos de negocios, ean internacional ha desarrollado, hace varios años, un sistema de números que garantiza la identificación única y exclusiva de productos y servicios. estos números proveen un lenguaje común donde fabricantes, exportadores, importadores, vendedores y reilers pueden comunicar información concerniente a su mercadería o al servicio que prestan.
<http://www.mygnet.com/pages/down.php?man=848>

Manejo de base datos**Novel completísimo**

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 402 KB
 Lo mejor paraustedes

<http://www.mygnet.com/pages/down.php?man=801>

Etapas del diseño del proceso de base de datos

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 262 KB
 Aquí esta todo amigos
<http://www.mygnet.com/pages/down.php?man=777>

Oracle**Iniciacion a oracle 8**

Franklin Escobar
franklinescobar@gmail.com

Tamaño: 580 KB
 Aquí mando un manual en pdf de oracle 8 para iniciar en bases de datos me parece muy completo no es de mi autoria es algo que encuentre por internet despues de mucho buscar espero les sea de ayuda
<http://www.mygnet.com/pages/down.php?man=814>

Manejo de base datos**Oracle**

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 39 KB
 Todo sobre oracle
<http://www.mygnet.com/pages/down.php?man=791>

Powerbuilder**Power builder 8, 9, 10 y 11**

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 4 MB
 El sexto de la saga de 6
<http://www.mygnet.com/pages/down.php?man=818>

Power builder ver 8, 9, 10 y 11

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 3 MB
 El quinto de la saga de 6
<http://www.mygnet.com/pages/down.php?man=817>

Power builder ver 8, 9, 10 y 11

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 2 MB
El cuarto de la saga de 6
<http://www.mygnet.com/pages/down.php?man=816>

Objetos y controles ver. 8 y 9

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 3 MB
Excelente manual para manipulación de controles y objetos
<http://www.mygnet.com/pages/down.php?man=813>

Powerscript parte 2 ver. 8 y 9

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 4 MB
Lenguaje de pb
<http://www.mygnet.com/pages/down.php?man=812>

Powerscript parte 1 ver. 8 y 9

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 12 KB
Lenguaje de pb
<http://www.mygnet.com/pages/down.php?man=811>

Referencia a datawindow parte1 ver. 8 y 9

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 2 MB
Esta es la referencia a la datawindow
<http://www.mygnet.com/pages/down.php?man=809>

Guia del usuario ver 8 y 9

Jaime Alfredo Aviles Flores
jaaf2000@gmail.com

Tamaño: 5 MB
Esta es la guia del usuario se ajusta a versiones 8 y 9 perfectamente
<http://www.mygnet.com/pages/down.php?man=808>

Varios**Manual de power builder 6.0 2 de 2**

Unkonw
mrojas@mavila.com.pe

Tamaño: 457 KB
Manual basico y muy util de power builder 6.0. espero que se sirva de ayuda.
<http://www.mygnet.com/pages/down.php?man=821>

Manual de power builder 6.0 1 de 2

Unkonw
mrojas@mavila.com.pe

Tamaño: 850 KB
Manual basico y muy util de power builder 6.0. espero que se sirva de ayuda.
<http://www.mygnet.com/pages/down.php?man=820>

Manejo de base datos**Manual de power builder**

Unkonw
mrojas@mavila.com.pe

Tamaño: 315 KB
Manual basico de power builder para principiantes
<http://www.mygnet.com/pages/down.php?man=819>

Redes**Construcción de antenas wifi**

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 347 KB
Muy bueno
<http://www.mygnet.com/pages/down.php?man=845>

Manual redes inalámbricas

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 782 KB
Muy bueno
<http://www.mygnet.com/pages/down.php?man=844>

Todo wifi

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 660 KB
Excelente guía
<http://www.mygnet.com/pages/down.php?man=843>

Vpn discovery tools

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 106 KB
Vpn discovery tools
<http://www.mygnet.com/pages/down.php?man=831>

Tecnología de cifrado

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 147 KB
Tecnología de cifrado verisign
<http://www.mygnet.com/pages/down.php?man=829>

Solución anti-phishing

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 55 KB
Solución anti-phishing de verisign
<http://www.mygnet.com/pages/down.php?man=828>

Autenticación y cifrado

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 275 KB
Autenticación y cifrado
<http://www.mygnet.com/pages/down.php?man=827>

Iniciación seguridad wifi completo

Gaizka
gaizkile@gmail.com

Tamaño: 1 MB
Conceptos a tener en cuenta a la hora de velar por la seguridad en una red wireless . ya lo siento por el fallo
<http://www.mygnet.com/pages/down.php?man=776>

Métodos de simulación**Redes**

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 81 KB
Es un para q puedan desarrollar de redes
<http://www.mygnet.com/pages/down.php?man=780>

Seguridad**Teraguar(tm) de verisign**

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 105 KB
Muy bueno
<http://www.mygnet.com/pages/down.php?man=841>

Security intelligence services

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 344 KB
Muy bueno
<http://www.mygnet.com/pages/down.php?man=840>

Verising identity protection

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 142 KB
Excelente
<http://www.mygnet.com/pages/down.php?man=839>

Verising identity protection español

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 65 KB
Excelente
<http://www.mygnet.com/pages/down.php?man=838>

Servicios managed firewall and virtual private network (vpn)

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 88 KB
Excelente
<http://www.mygnet.com/pages/down.php?man=837>

Servicio managed intrusion detection system

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 54 KB
Excelente
<http://www.mygnet.com/pages/down.php?man=836>

Introducción a las pruebas de vulnerabilidad de red.

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 93 KB
Vulnerabilidades
<http://www.mygnet.com/pages/down.php?man=835>

Estrategias para telecomunicaciones.

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 187 KB
Excelente
<http://www.mygnet.com/pages/down.php?man=834>

Estrategias eficaces de gestion y riesgos.

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 115 KB
Excelente manual
<http://www.mygnet.com/pages/down.php?man=833>

Digital id

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 97 KB
Por verising
<http://www.mygnet.com/pages/down.php?man=832>

Documentos xml**Xml key management**

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 328 KB
Por vereising
<http://www.mygnet.com/pages/down.php?man=830>

Software**Manual de ds**

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 26 KB
Manual de dos
<http://www.mygnet.com/pages/down.php?man=795>

Trucos**Novell**

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 51 KB
Cerrar cesión imprimir y etc
<http://www.mygnet.com/pages/down.php?man=800>

Vb**Programación de macros para botones de word**

Luis
buitre103@hotmail.com

Tamaño: 95 KB
El manual describe paso a paso cómo crear mediante macros botones que pueden incrustarse en el propio word para obtener las funciones de convertir texto a mayúsculas y a minúsculas (opciones no aportadas en word2000)
<http://www.mygnet.com/pages/down.php?man=868>

Virus y troyanos**Winsock**

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 122 KB
Este es un pequeño manual que supongo que ya lo habrán visto en el Internet ya que en cualquier pagina de programación se lo consigue, este manual es una pequeña introducción a control winsock, con un ejemplo.
<http://www.mygnet.com/pages/down.php?man=867>

Introducción a los virus 2

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 85 KB
Este manual es halgo semejante al anterior pero vale la pena ponerlo.
<http://www.mygnet.com/pages/down.php?man=864>

Introduccion a los virus

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 89 KB
Este pequeño manual sobre la creación de los virus le ayudara a comprender los conceptos básicos de programación de virus.
<http://www.mygnet.com/pages/down.php?man=863>

Troyanos en visual basic

Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 737 KB
Como crear un pequeño troyano, está muy bien explicado y es muy bueno, ya que casi no se consigue en el Internet.
<http://www.mygnet.com/pages/down.php?man=862>

Vc

Crear dll vers.1

Joseph
elprogramador83@hotmail.com

Tamaño: 785 KB
 Manual para crear y utilizar una dll en visual c++ y dev-c
<http://www.mygnet.com/pages/down.php?man=869>

Windows

Guia rapida de windows 2003 server

Cesar Gutierrez
cesar.leandro@gmail.com

Tamaño: 1 MB
 Excelente
<http://www.mygnet.com/pages/down.php?man=842>

Manual de la evolución de Windows

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 162 KB
 Evolución
<http://www.mygnet.com/pages/down.php?man=797>

Manual de computadoras

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 3 MB
 Lo mejor de lo mejor
<http://www.mygnet.com/pages/down.php?man=794>

Win98

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 2 MB
 Win98
<http://www.mygnet.com/pages/down.php?man=789>

Manual de windows 98

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 2 MB
 Manual de windows 98
<http://www.mygnet.com/pages/down.php?man=782>

Manual de windows xp

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 1 MB
 Manual de Windows xp para novatos
<http://www.mygnet.com/pages/down.php?man=781>

Registro de Windows

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 25 KB
 Registro de windows algunos trucos con esto y para que sirve los mas principales
<http://www.mygnet.com/pages/down.php?man=847>

La bios

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 21 KB
 Resumen, lo básico de la bios
<http://www.mygnet.com/pages/down.php?man=846>

Movie maker manual

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 190 KB
 Movie maker
<http://www.mygnet.com/pages/down.php?man=802>

Win 2000

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 22 KB
 Todo sobre win 2000
<http://www.mygnet.com/pages/down.php?man=792>

Archivos y directorios**Evolcion de windows**

Christian Palacios Socualaya
cri1987_9@hotmail.com

Tamaño: 162 KB
 Evolución
<http://www.mygnet.com/pages/down.php?man=799>

Navegadores**Manual de iis**

Alejandro Adrián Ponicke
no lo tengo@.com

Tamaño: 2 MB
 Soluciones microsoft para profesionales it guía de seguridad para internet information services 6.0 autor: alejandro adrián ponicke mcsa, mcse, mct
<http://www.mygnet.com/pages/down.php?man=798>

Enlaces en el mes

Asp.net

Howto de net

Enviado por Shakba

A diferencia de otros tutoriales que se supone que hay que leer desde el principio hasta el final, esta sección se puede utilizar como referencia temática.

<http://es.gotdotnet.com/quickstart/howto/>

C#

Itext para .net

Enviado por Landanohr

Versión de la librería itext para la plataforma .net

<http://itextsharp.sourceforge.net/>

Css

Herramientas para desarrolladores

Enviado por Alfredo De Jesús Gutiérrez Gómez

Encontraras una serie de herramientas para desarrolladores ordenadas por categorías. entre ellas hay herramientas orientadas a css (páginas web donde encontrar la inspiración...), herramientas para javascript, para el lenguaje de moda (ajax), php, flash, hasta para ruby (lenguaje que parece tener cada vez más presencia en el mercado y que se deberá seguir de cerca....

<http://www.tonyyoo.com/protolize/>

Delphi

30 chuletas para desarrolladores

Enviado por Alfredo De Jesús Gutiérrez Gómez

entre estos recursos siempre puede haber alguno que nos venga bien

<http://www.petefreitag.com/item/455.cfm>

Boletín pascal para programadores de delphi y kilix

Enviado por Alfredo De Jesús Gutiérrez Gómez

El boletín pascal es una publicación no periódica (casi quincenal) totalmente gratuita* que se distribuye por email en formato de texto plano, lo que lo hace muy compacto y además permite que se pueda leer directamente con cualquier programa de mail o desde cualquier servicio de web mail sin necesidad de programas adicionales.

<http://www.latiumsoftware.com/es/pascal/index.php>

Diseño Gráficos

Crear logo

Enviado por Christian Palacios Socualaya

Q más

<http://www.soslogodesign.com/disenodelogo.html>

Diseño Web

Herramientas para blog

Enviado por Alfredo De Jesús Gutiérrez Gómez

Probblogger nos ofrece un listado con 55 herramientas para blogs. entre ellas encontraréis paquetes para estadísticas, editores de blogs, news aggregators, suscripciones por e-mail, y muchas otras herramientas. os recomiendo que le hechéis un vistazo, siempre se descubren recursos interesantes.

<http://www.probblogger.net/archives/2006/04/15/blog-tools/>

Crea tus banner

Enviado por Christian Palacios Socualaya

Crea tus propios banners

<http://www.bannerbreak.com/>

Letras para tu pagina

Enviado por Christian Palacios Socualaya

Letras para tu pagina web esta interesante

<http://www.letrasanimadas.com/>

Musica para tu pagina

Enviado por Christian Palacios Socualaya

Music midi para tu pagina

<http://www.nurisite.com/midisonly/index.htm>

Diseñador de logos

Enviado por Christian Palacios Socualaya

Amigos aqui les trigo un diseñador degraficos y letras

<http://cooltext.com/>

Un diseñador gratis

Enviado por Christian Palacios Socualaya

Es un diseñador solo tines q hacer es saber solo un poco de paginas nada mas

www.palimpalem.com

Pdfs de flash 8

Enviado por Jesús F. Bárcena

Todos los pdfs de flash, pesa mas de 5 megas , por eso no lo pude subir, es excelente.

<http://www.adobe.com/support/documentation/es/flash/>

Internet

Ajax

Enviado por Douglas Quintero Vines

Este es un pequeño artículo que explica la nueva tecnología web ajax, esta en ingles pero realmente es bueno que lo lean

<http://www.adaptivepath.com/publications/essays/archives/000266.php>

Java

Full netbeans magazine issue one

Enviado por Gerardo Ángeles Nava

(34.5mb) 68 pages including: 7 articles, netbeans day information and activities at 2006 javaone conference

http://www.netbeans.org/download/magazine/01/nb01_web.pdf

Linux**Herramientas veteranas**

Enviado por Alfredo De Jesús Gutiérrez Gómez

La noticia está en que la compañía canadiense corel acaba de adquirir winzip computing cuyo precio fue de 4,3 millones de acciones ordinarias de corel. esta acción supone el fin de su sistema de distribución, ya que a partir de ahora no podremos descargarnos, como hasta ahora, la versión de evaluación.

<http://www.elmundo.es/navegante/2006/05/04/empresas/1146733209.html>

Mysql**Mysql wokbench**

Enviado por Shakba

Herramienta visual de diseño de bases de datos, evolución del anterior dbdesigner4

<http://barrapunto.com/article.pl?sid=06/04/26/1121241>

Varios**Camaleon css**

Enviado por Douglas Quintero Vínces

En esta pagina podra ver el poder de css al separar el contenido de una pagina web con la presentacion

<http://www.camaleoncss.com/1/p1/camaleon.html>

Tutórales de programación

Enviado por Douglas Quintero Vínces

Aqui encontraras buenos tutoriales y recursos de lenguajes de programación

<http://www.programmingtutorials.com/>

Tutorial crystal report

Enviado por Douglas Quintero Vínces

En esta pagina esta un buen tutorial de crystal report reviselan.

<http://www.insightdirect.com/docs/crystal/>

Zonnon

Enviado por Gustavo Alberto Rodriguez

Nuevo lenguaje de programación para .net

<http://www.zonnon.ethz.ch/index.html>

Varios how-to excelentes

Enviado por Jonathan Granade

Antes que nada, hola a todos, esta es mi primer humilde colaboracion, no la encuentre en el resto de los enlaces, y me parece que es muy util. algunos conoceran el sitio tldp.org (the linux documentation proyect), se trata de una serie de how-to's de variados sabores...desde redes hasta comandos del sistema, etc. creo que no hay que dejar de consultarlo a la hora de tener algun problema. nota: estos how to no son de programacion, son de tareas variadas.

<http://www.tldp.org/howto/howto-index/categories.html>

Código fuente y manuales

Enviado por Diego Trujillo

Todo sobre programación de c/c++, código fuente, etc.

<http://www.elrincondelc.com>

Manuales

Enviado por Christian Palacios Socualaya

Mejores manuales

http://www.solomanuales.org/manuales_arquitectura_de_la_inf_ormacion-manuall214708.htm

Wikilearning

Enviado por Shakba

En wikilearning podéis encontrar cientos de tutoriales de los más diversos temas, pero lo que hace de wikilearning diferente es que, al tratarse de un wiki, cualquier usuario puede colaborar para hacer cada tutorial más y más rico.

<http://www.wikilearning.com/>

Gotapi referencias de lenguajes en un solo lugar

Enviado por Shakba

Si eres programador o estás aprendiendo algun lenguaje este sitio te va encantar, se llama gotapi y es una interface donde se leen referencias de distintos lenguajes desde html, css, pasando por xml, mysql hasta php. todo comando, funcion, tag, etc, ordenado y accesible desde una sola interface.

<http://www.gotapi.com/>

Seguridad**Www.perantivirus.com**

Enviado por Christian Palacios Socualaya

Www.perantivirus.com

www.perantivirus.com

Vb.net**Versiones express de vs2005 y sql server 2005 (gratis)**

Enviado por Juan Francisco Berrocal

Descarga la nueva linea de productos de desarrollo express, es gratis

<http://www.microsoft.com/spanish/msdn/vstudio/express/default.t.mspx>

Programar.net

Enviado por Juan Francisco Berrocal

Recursos y aprendizaje de .net

<http://www.programar.net/>

Wap**Tagtag.com**

Enviado por Pedro Ernesto

Hospedaje wap, ringtones, gráficos, aplicaciones j2me para el celular

<http://tagtag.com/site/index.php3>