Sistema de Archivos Criptográfico bajo Linux (CFS) COMO

Copyright (C) 1996 Alexander O. Yuriev, alex@bach.cis.temple.edu
Traducido por Salvador Fernández Barquín sferbar@internetica.net.mx Marzo 14, 1996

Este documento describe cómo compilar, instalar y configurar CFS, el Cryptographical File System.

Índice General

1 Introducción

Este documento describe cómo compilar, instalar y configurar CFS, que fue escrito por Matt Blaze de AT&T, bajo Linux.

2 Copyright

La siguiente nota de copyright, copiada directamente de CFS 1.12 describe las restricciones sobre el uso de CFS:

El autor de este software es Matt Blaze. Copyright © 1992, 1993, 1994 por AT&T. Se permite usar, copiar, y modificar este software sin necesidad de permiso expreso, con la condición que este aviso sea incluido íntegramente en todas las copias del software tal y como está en todas las copias o modificaciones de este software, así como en todas las copias de la documentación de soporte para dicho software.

Este software está sujeto a los controles de exportación de los Estados Unidos. No está permitido exportarlo, en su totalidad o en parte, por cualquier motivo o permitir cualquier exportación, por medio de acto u omisión, sin previa autorización de parte del gobierno de los Estados Unidos y permiso escrito de AT&T.

En particular, usted no debe hacer disponible cualquier parte de este software para distribución general o no restringida a otros, o no debería usted revelar este software a personas diferentes a los ciudadanos y residentes permanentes de los Estados Unidos y Canadá.

ESTE SOFTWARE SE PROVEE "TAL CUAL", SIN NINGUNA GARANTÏA EXPRESA O IMPLICADA. EN PARTICULAR, NI LOS AUTORES NI AT&T HACEN NINGUNA REPRESENTACION O GARANTÍA DE NINGÚN TIPO CONCERTANDO LA MERCANTILIDAD DE ESTE SOFTWARE O SUS PROPÓSITOS PARA ALGÚN PROPÓSITO EN PARTICULAR.

A pesar que la información en este documento es considerada como correcta, ni el Autor ni los Laboratorios CIS, o la Universidad Temple da ninguna clase de GARANTÍAS y no es o se hace responsable de lo que pueda pasar si usted sigue esta guía. La información en este documento se proporciona TAL CUAL!.

3 ACERCA DE CFS

CFS proporciona una aplicación independiente de encriptación-desencriptación de la capa del sistema de archivos que no requiere modificación del código principal del sistema de archivos o ninguna clase de modificación del código del kernel.

El seguro simétrico implementado en la versión del flujo principal del CFS está basado sobre un seguro DES modificado, ejecutándose en modo CBC haciendo un ataque de fuerza bruta en contra del usual espacio de llave DES, no real de 56 bits.

La estructura del CFS realiza un remplazo del flujo principal del seguro DES con un Fast-DES o algún otro seguro simétrico que provea un proceso extremadamente seguro. Por favor refiérase al "*White paper*" referente al CFS para más información. `ftp://bach.cis.temple.edu/pub/Papers/cfs.ps`

4 Compilación e instalación de CFS.

CFS no se compila tal y como viene sobre Linux. Las siguientes instrucciones le llevarán a conseguir que CFS se ejecute en su sistema Linux. Hay diversos métodos para hacer que CFS trabaje en Linux, el más limpio de ellos es el basado sobre las modificaciones de Olaf Kirch. Su versión de CFS esta disponible en

`ftp://ftp.mathematik.th-darmstadt.de/pub/linux/okir/cfs-1.1.2.tar.gz`

Olaf firmó el archivo modificado. La firma PGP de la versión modificada del `cfs-1.1.2` puede ser obtenida de `ftp://ftp.mathematik.th-darmstadt.de/pub/linux/okir/cfs-1.1.2.pgp`

En modo mono-usuario, se compila CFS usando la instrucción "`make`".

Después de la compilación, instale `cfsd`, `cdetach`, `ccat`, `cmkdir`, `cname` y `cattach` en el directorio `/usr/local/sbin` con propietario-grupo `root.wheel` y el modo de acceso `551`.

Genere una lista de hashes MD5 de los binarios limpios. Copie estos archivos junto con el `md5sum` a un medio tal como un CD o un disquete y protéjalo contra escritura.

Cree el directorio `/.cfsfs`, el cual será usado como un gancho por el servidor CFS. Cree este directorio como dueño `root.root` y protegido con el modo de acceso "000". Cree el directorio `/securefs`, el cual se convertirá en la raíz del árbol de CFS.

Añada las siguientes líneas a su `/etc/rc.d/rc.local`:

```
            echo -n "Inicializando sistema de ficheros encriptado: "
    if [ -x /usr/local/sbin/cfsd ]; then
            /usr/local/sbin/cfsd > /dev/null
```

```
                echo -n "cfsd "
        /bin/mount -o port=3049,intr localhost:/.cfsfs /securefs
                echo -n "loopback "
        echo "done"
else
           echo "No se ha instalado el sistema de ficheros encriptado"
        fi
```

Los usuarios de las distribuciones Caldera Network Desktop y Red Hat Commercial Linux deben añadir el archivo `cfsfs` que está incluído al final de este documento en su directorio `/etc/rc.d/init.d`. Realice un enlace simbólico, `S65cfsfs` de éste en los directorios apropiados al nivel de ejecución usando la instrucción:

```
ln -s ../init.d/cfsfs S65cfsfs
```

en `/etc/rc.d/rcX.d`, donde `X` es el número de nivel de ejecución (`init`), añada la línea:

```
/.cfsfs         localhost
```

en `/etc/exports`. Finalmente, añada la línea:

```
portmap: 127.0.0.1
```

al el archivo `/etc/hosts.allow`.

Reinicie su computadora. Esta entrará en modo multiusuario. Ejecute el comando `mount` para verificar que CFS esté corriendo. Si todo esto fue superado con éxito, verá una nueva línea en el lista de los sistemas de archivos:

```
localhost:/.cfsfs on /securefs type nfs (rw,port=3049,intr,addr=127.0.0.1)
```

5 Creación del directorio CFS.

Para crear un directorio CFS protegido llamado `secreto` use el comando

```
cmkdir secreto
```

Le pedirá que la frase de paso y que la verifique. Si sale bien, un nuevo directorio llamado `secreto` aparecerá en el directorio actual. Este directorio contendrá información encriptada la cual no será accesible, sólo lo será en el caso de que éste esté añadido al árbol del CFS.

Para ordenar que el directorio `secreto` se añada a la lista de directorios administrados por CFS, este ha de ser añadido a el árbol CFS usando la instrucción:

```
cattach secreto Gran-Secreto
```

CFS requerirá que escriba la frase de paso para el acceso. Si ésta coincide con la frase de paso proporcionada a la instrucción `cmkdir` que creó el directorio originalmente, la información en el directorio secreto será accesible de forma no encriptada bajo `/securefs/Gran-Secreto` al usuario que proporcionó la frase de paso correcta. Note que usualmente toma cerca de un minuto añadir el directorio protegido al árbol del CFS. Cuando el usuario ha terminado de manipular la información debe utilizar la instrucción:

```
cdetach Gran-Secreto
```

Para destruir la llave de acceso. Esta instrucción elimina el directorio `secreto` de la lista de directorios administrados por CFS haciendo imposible acceder a la información en forma de texto plano en este directorio hasta que nuevamente sea añadido usando la instrucción `cattach`.

6 Protección del CFS.

Para conceder acceso a un usuario a partes encriptadas del árbol de directorios, CFS necesita que el usuario proporcione la frase de paso que es usada para generar un conjunto de llaves de acceso. Una vulnerabilidad de una frase de paso, permitirá a un intruso acceder a la información encriptada a través del modulo de seguridad Unix.

Por ello, es extremadamente importante proteger el acceso a las frases de paso. Hay dos maneras básicas que pueden ser utilizadas por los intrusos para obtener su frase de paso. Son:

1. Ataques con *Sniffers*
2. Ataques contra el protocolo.

Las siguientes instrucciones pueden ser utilizadas para minimizar la posibilidad de un ataque exitoso contra CFS:

1. Asegurar que los binarios de CFS no estén comprometidos de ninguna forma.
2. Asegurar que `cattach`, `ccat`, `cmkdir`, `cname`, el servidor CFS `cfsd` y finalmente, `cdattach` no serán sustituidos por versiones "*troyanas*" que capturen las frases de paso o, en el caso del `cfsd`, las llaves de acceso.
3. Asegurar que el Servidor CFS no esté comprometido de modo que no se realice el procedimiento de encriptación correctamente.
4. Un ataque contra `cdeattach` usualmente involucra una pequeña modificación que evita la correcta destrucción de las llaves de acceso, permitiendo a un intruso obtener acceso a una parte supuestamente separada del árbol de directorios.
5. La manera más simple para asegurar que los binarios no sean comprometidos es compilarlos estáticamente y guardarlos en un CD. Otra manera es compilar estáticamente los binarios, usar `md5sum`, la calculadora de procesado de mensaje (`message-digest`) y escribir los hashes MD5 en un medio protegido contra escritura.

   Antes de usar alguno de los programas de CFS sobre un sistema, monte un disquete y compare los hashes MD5 de los binarios del sistema con los hashes de las copias limpias compiladas estáticamente, localizadas en el disquete, sustituyendo las versiones comprometidas.
6. Capturadores de teclado usados para capturar las frases de paso, tal como los usuarios las van tecleando. Dependiendo de las circunstancias, muchos usuarios no son lo bastante cuidadosos ignorando las siguientes indicaciones:
   (a) Cuando escriba una frase de paso en una `xterm`, asegurar que el programa `xterm` no está comprometido y use la opción "Teclado seguro" mientras se escribe la frase de paso. Esto previene que las pulsaciones sean interceptadas por capturadores X-Window.
   (b) Escriba las frases de paso desde la terminal conectada directamente a un puerto serie del sistema cuando dicha terminal esté disponible.
   (c) Cerciórese de que sus permisos en `ptys` y `ttys` no permitan a otros la lectura de tus pulsaciones directamente del dispositivo.
7. Nunca escriba su frase de paso a través de la red, aunque la red esté localizada tras un cortafuegos y confíe en que todos los que están conectados a su red no usen sniffers. Esto es aplicable también a redes que usen routers seguros (scrambling routers), porque no hay garantía en absoluto que los routers usen un encriptamiento sólido o no tengan una puerta trasera o un agujero de seguridad que potencialmente pueda permitir a un intruso anular la encriptación usada por el router. Si tiene que escribir su clave de acceso a través de la red, hágalo solamente si está usando un canal encriptado entre sistemas tal como el creado por el protocolo `deslogin(8)`.

8. Los árboles protegidos CFS deben ser desligados siempre (`de-attach`) del sistema de archivos cuando no sean usados, aun cuando vaya a dejar su sistema "sólo" por un par de minutos.

7 Problemas conocidos de CFS

Hasta este momento sólo se conoce un problema que puede ser reproducido. El error de "`Permission denied`" que se genera cuando un usuario intenta acceder a archivos localizados en un disco compacto.

8 Créditos (Documento en inglés).

Las siguientes personas ayudaron en el proceso de preparación de este documento: Topher Hughes del Colegio Dickinson, Elie Rosenblum del Montgomery Blair High School, Mario D. Santana de la Universidad del Estado de Florida, Daniel P. Zepeda y Olaf Kirch.

9 Nota de la traducción.

Mi nombre es Salvador Fernández Barquín, formo parte del proyecto LUCAS/INSFLUG. Este documento es mi aportación para que el proyecto Linux sea cada vez más grande y conocido entre nosotros los que hablamos la lengua de Cervantes; ahora que la seguridad en los servidores de Internet (y Linux en particular) es un tema importante para todo administrador o usuario de Linux, consideré esta una solución muy interesante de aplicar.

Particularmente, espero que este documento sea de ayuda e interés a todos aquellos que deseen implementar un esquema de seguridad a nivel sistema de archivos en su Linux.

Hay mucho por traducir, así como también hay muchos documentos traducidos, visite `http://www.infor.es/LuCAS` o o sus múltiples espejos para conocer más sobre este proyecto o obtener otros documentos en castellano.

No está de más decir que intentado ajustarme totalmente al original de Alexander O. Yuriev y he revisado la traducción un par de veces. No obstante aún puede quedar algo por pulir o se me ha podido colar alguna errata, de cuya responsabilidad me hago cargo, pero jamás del buen o mal uso que pueda derivar la lectura de este documento.

Para cualquier comentario, errata o consulta sobre la traducción, mándeme un mensaje electrónico a: `sferbar@internetica.net.mx`.

Un saludo y buen provecho

Salvador Fernández Barquín.

10 scripts

```
#!/bin/sh
#
# $Header: /Secure/secure-doc/linux/CFS/RCS/CFS-Doc,v 1.4 1996/03/15 04:49:37 alex Exp alex $
#
# cfsfs         Crypto filesystem
#
# Author:       Alexander O. Yuriev <alex@bach.cis.temple.edu>
#               Derived from cron
```

```
# Cargamos la librar\'{\i}a de funciones.
. /etc/rc.d/init.d/functions

# Averiguamos c\'{o}mo se nos ha ejecutado.
case "$1" in
 start)
        echo -n "Arrancando sistema de ficheros encriptado: "
        if [ -x /usr/local/sbin/cfsd ]; then
                /usr/local/sbin/cfsd > /dev/null
                /bin/mount -o port=3049,intr localhost:/.cfsfs /securefs
                echo "listo"
        else
                echo -n "El sistema de ficheros encriptados no ha sido iniciado"
        fi
        touch /var/lock/subsys/cfsfs
        ;;
 stop)
        echo -n "Deteniendo sistema de ficheros encriptado: "
        umount /securefs
        killproc cfsd
        echo
        rm -f /var/lock/subsys/cfsfs
        ;;
 *)
        echo "Empleo: cfsfs {start|stop}"
        exit 1
esac

exit 0
```

11 Anexo: El INSFLUG

El *INSFLUG* forma parte del grupo internacional *Linux Documentation Project*, encargándose de las traducciones al castellano de los Howtos (Comos), así como la producción de documentos originales en aquellos casos en los que no existe análogo en inglés.

En el **INSFLUG** se orienta preferentemente a la traducción de documentos breves, como los *COMOs* y *PUFs* (**P**reguntas de **U**so **F**recuente, las *FAQs*. `:)`), etc.

Diríjase a la sede del INSFLUG para más información al respecto.

En la sede del INSFLUG encontrará siempre las **últimas** versiones de las traducciones: `www.insflug.org`. Asegúrese de comprobar cuál es la última versión disponible en el Insflug antes de bajar un documento de un servidor réplica.

Se proporciona también una lista de los servidores réplica (*mirror*) del Insflug más cercanos a Vd., e información relativa a otros recursos en castellano.

Francisco José Montilla, `pacopepe@insflug.org`.