SEGURIDAD EN LOS SISTEMAS COMPUTACIONALES
una opción para la familia BTOS.

Freddy Abarca R.*

RESUMEN

Con la inquietud de brindar más seguridad a las aplicaciones diseñadas en el ambiente BTOS, el presente artículo plantea un procedimiento sencillo que, haciendo uso de la analogía "cerradura y llave", concibe a la biblioteca principal del sistema operativo, como "cerradura" y, a un disco flexible con especificaciones precisas, como "llave".

1. INTRODUCCION

Dadas las facilidades que día a día ofrece la tecnología en el campo de las comunicaciones, la intromisión no controlada de usuarios de aplicaciones a sistemas computacionales ya establecidos, es, sin lugar a dudas, la principal fuente de preocupación para los administradores de estos centros. En este contexto, el objetivo del presente trabajo es precisamente someter a consideración del administrador una opción de seguridad para los sistemas de aplicación desarrollados bajo el ambiente BTOS.

A pesar de que no es objeto de este artículo comparar los niveles de seguridad de los distintos ambientes en que se pueden desarrollar sistemas, sí se desea dejar constancia de la extraordinaria flexibilidad y confiabilidad del *hardware* y del *software* de la familia de los BTOS. Por otra parte, se comparte el criterio de que los sistemas de información desarrollados en BTOS tienen un peligro latente: una vez conocida la clave de ingreso de un usuario cualquiera con la respectiva palabra clave, los programas de aplicaciones se abren totalmente a terceras personas en un radio de acción que se extiende en función del conocimiento de la palabra clave. Esta última particularidad se debe al diseño de la estructura jerárquica de las protecciones del BTOS, que por otro lado y paradójicamente, constituye una herramienta muy útil en el diseño de esas aplicaciones.

* Centro de Investigaciones en Computación. Instituto Tecnológico de Costa Rica.

2. UN DISCO FLEXIBLE LLAVE

Sin olvidar las medidas tradicionales que acompañan la literatura en cuanto a seguridad se refiere, el fundamento de la idea sobre la cual se desarrolla este artículo es sumamente sencilla: se basa en la misma existente entre los conceptos "cerradura" y "llave" a la que todos estamos familiarizados.

Se hará la siguiente analogía: "cerradura" con la biblioteca principal del sistema, y "llave" con "un disco flexible" con especificaciones que se expondrán posteriormente. En otras palabras, si un usuario regular desea trabajar sin la autorización respectiva y no dispone del "Disco Flexible Llave", los archivos residentes en biblioteca principal no podrán activarse al menos por métodos convencionales.

3. NOMENCLATURA BASICA

Se partirá de una configuración estándar en donde el sistema operativo resida en el nodo {N1}, el volumen [SYS], y en biblioteca <SYS>. A esta biblioteca se le denominará "biblioteca principal". El administrador deberá hacer los cambios pertinentes en las especificaciones que se recomiendan si, por ejemplo, el sistema operativo reside en un volumen denominado [!DO], o [WIN], o como sea el caso. (En aras de una mejor lectura del presente artículo la variable "nodo" se dejará de lado a partir de este momento). Se

supondrá además que los archivos con las especificaciones de los usuarios residen en la dirección [SYS] <SYS> como es lógico esperar.

Asimismo, se partirá de la nomenclatura [FO] para especificar la unidad de disco flexible, el nombre del volumen del disco flexible "ARCHIVE", y las instrucciones y mandatos ("commands") se anotarán en idioma inglés para evitar conflictos de traducción.

4. PASOS POR SEGUIR

Se pensará que existen tres usuarios, denominados "A", "B" y "C" a quienes el administrador les desea inhibir el ingreso al sistema a partir de cierto momento o por cualquier razón que el administrador estime conveniente. Si se desea poner en práctica este sistema de seguridad, deben seguirse los siguientes pasos.

Primero

En la biblioteca principal, crear un archivo sencillo con el nombre de "[SYS] <SYS>LISTA. USUARIOS" utilizando el editor de textos. En este archivo se escribirán los nombres de los usuarios del sistema a quienes se les desea obtaculizar precisamente el ingreso.

```
EDIT

[File]                          LISTA.USUARIO
[Your Name]
```

de forma tal que el archivo se lea así:

```
A.USER B.USER C.USER
```

Segundo

En la biblioteca principal genere un archivo de usuario con nombre "[SYS]<SYS>SEGURIDAD.USER" que tenga las siguientes especificaciones:

```
:SignOnVolume:FO
:SignOnDirectory:SYS
:SignOnPassword:
:SignOnFilePrefix:
:SignOnExitFile:[FO]<SYS>SIGNON.RUN
:ExecCmdFile:SYS.CMDS
:SignonChainFile:LCOPY.RUN LCOPY
A.USER B.USER C.USER
[FO]<SYS>
[SYS]<SYS>
```

Obsérvese que el contenido del archivo "[SYS]<SYS>LISTA.USUARIOS" coincide con la lista bajo la instrucción "LCOPY" de "[SYS]<SYS>SEGURIDAD.USER". Se sabe que la meta buscada pudo haberse efectuado más eficientemente por otras opciones, pero se recomienda esta forma como una medida de prevención extra al administrador. Nótese también cómo el usuario "[SYS]<SYS>SEGURIDAD.USER" no aparece ni en el propio usuario "[SYS]<SYS>SEGURIDAD.USER" ni en la lista "[SYS]<SYS>LISTA.USUARIOS"

Tercero

Generar una nueva instrucción en el archivo "[SYS]<SYS>SYS.CMDS" con el nombre "CANDADO" el cual se encargará de borrar de la biblioteca principal los archivos de usuarios especificados en "[SYS]<SYS>LISTA. USUARIOS" En otras palabras, una vez ejecutada la instrucción "CANDADO" los usuarios "A", "B" y "C" no pueden ingresar al sistema. Este paso debe hacerse de la siguiente manera:

```
NEW COMMAND

Command Name CANDADO
Run File !3
[File Names] 'Borrar Archivos Usuarios. Dar
@LISTA.USUARIOS'
[Description] 'Borrar Archivos de Usuarios'
[Overwrite?]
[Case]
[Command File]
```

Cuarto

Inicializar un disco flexible que se denominará "Disco Llave".

Quinto

Grabar desde la biblioteca principal al "Disco Llave" los archivos SIGNON.RUN LCOPY.RUN de esta manera:

```
LCOPY

[File List]                SIGNON.RUN LCOPY.RUN
[File Prefix(es) From]     [Sys]<Sys>
[File Prefix(es) To]       [FO]<Sys>
[File Suffix(es)]
[Overwrite OK?]
[Confirm Each?]
[Continue on Error?]
[Verify Copy?]
```

Sexto

Como último paso, grabar en el "Disco Llave" los archivos de usuarios residentes en la biblioteca principal a quienes se les desea inhibir el ingreso al sistema una vez ejecutada la instrucción "CANDADO". En otras palabras,

```
LCOPY

[File List]                @Lista.Usuarios
[File Prefix(es) From]     [Sys]<Sys>
[File Prefix(es) To]       [FO]<Sys>
[File Suffix(es)]
[Overwrite OK?]
[Confirm Each?]
[Continue on Error?]
[Verify Copy?]
```

Sétimo

Hasta este punto del procedimiento, la bitácora del disco flexible que actuará como llave debe leerse de una forma similar a:

FLOPPY DISK PRINT FILE

Length Sectors	Last Modified	Protec
[ARCHIVE]<SYS>A.USER	145	1 Nov 10, 1988 1:38 PM 15
[ARCHIVE]<SYS>B.USER	145	1 Nov 10, 1988 1:38 PM 15
[ARCHIVE]<SYS>C.USER	145	1 Nov 10, 1988 1:39 PM 15
[ARCHIVE]<SYS>SIGNON.RUN	36777	72 Nov 10, 1988 2:11 PM 15
[ARCHIVE]<SYS>LCOPY.RUN	21417	42 Nov 14, 1988 5:56 PM 15
[ARCHIVE]<sys>fileHeaders.sys	98304	192 Nov 10, 1988 1:24 PM 15
[ARCHIVE]<sys>crashDump. sys	0	0 Nov 10, 1988 1:24 PM 15
[ARCHIVE]<sys>mfd.sys	512	1 Nov 10, 1988 1:24 PM 15
[ARCHIVE]<sys>sysImage.sys	0	0 Nov 10, 1988 1:24 PM 15
[ARCHIVE]<sys>log.sys	0	0 Nov 10, 1988 1:24 pm 15
[ARCHIVE]<sys>badBlk.sys	512	1 Nov 10, 1988 1:24 PM 15

Total sectors: 311

5. ACTIVACION DEL PROCEDIMIENTO

Primero

Desde el ejecutivo, y en el momento que el administrador lo considere conveniente, accionar la instrucción "CANDADO" cediéndole la expresión "@ LISTA.USUARIOS", de esta forma:

CANDADO

[Borrar Archivos Usuarios. @ Dar LISTA.USUARIOS]
Lista.Usuarios

Segundo

Para permitir el ingreso nuevamente a los usuarios inhibidos para ello, utilizar el usuario "SEGURIDAD". Será evidente que el sistema urge del "Disco Llave" para recuperar información: se notará cómo el sistema recupera los archivos de usuarios borrados con la instrucción 'CANDADO'.

Tercero

Deposite el "Disco Llave" en un lugar seguro. Todas las ventajas y desventajas que implica disponer de una llave para un cerrojo en una situación dada, son válidas para la idea desarrollada en este artículo. Si la necesidad de una llave es perentoria, se reitera la necesidad de disponer de copias por razones obvias de olvido, destrucción, o maltrato, a no ser que el administrador deje "usuarios" con nombres inaccesibles para casos extremos, lo que, personalmente, se recomendaría.

REFERENCIAS CONSULTADAS

1. UNISYS. **BTOS Standard Software Operations Guide**. E.E.U.U., Febrero de 1987.

2. UNISYS. **BTOS, Reference Manual.** E.E.U.U., Febrero de 1986.