FTPSERV-E

Product Overview

17. September 1999

GreenHouse
Software & Consulting
Karl-Heinz Weber
Heinrichstraße 12
D-45711 Datteln/Horneburg
Germany

The Problem

It is not a security breach to connect a Tandem system to a TCP/IP network, but it may cause security related problems.

Accessing a Tandem system, either through TELNET or FTP, always requires the requesting user to present their system known ID and corresponding password for authentication.

However, it might be necessary to restrict specific users from accessing the system through FTP, or from accessing (import, export) specific files through FTP. Maybe a user should get access to FTP without having valid GUARDIAN credentials (ID and password). Perhaps you need to allow the establishment of a FTP session only from specific IP addresses. You may want to log FTPSERV activities without the need to configure Safeguard Access Control Lists (ACLs), or you may want to send dependent triggers to other programs/servers to start processing when a file is received or transmitted.

The following features would be required in the standard FTPSERV program to make it accommodate these situations:

1. Control of system users (GUARDIAN and Alias users), accessing FTP
2. Ability to grant access to FTP for generic users (non GUARDIAN users)
3. Control of disk files that system users and generic users are allowed to access
4. Check of IP address, establishing a FTP session
5. Audit of all security related FTPSERV events
6. Optional support for dynamic passwords (TimeToken)
7. Event-based message generation

The FTPSERV-E Solution

*Green*House *Software and Consulting* has designed a special library for the standard FTPSERV product, making it a security enhanced version (FTPSERV-E). The library adds features to the standard functionality, and allows complete control of FTP.

FTPSERV-E is a ready to run product which matches the most current version of the standard FTPSERV.

The FTPSERV-E features are realized through ENSCRIBE type files maintained by a PATHMAKER application that comes with FTPSERV-E.

1. FTPEFILE (Disk file control)
2. FTPEUSER (System user control [GUARDIAN and Alias User])
3. FTPEUMAP (Generic user control)
4. FTPEUMSG (User defined event messages)
5. FTPEIPAD (Global IP addresses)
6. FTPEIPUR (User specific IP addresses)
7. FTPEFAST (FTPSERV-E configuration)

FTPSERV-E Log

All security related actions of FTPSERV-E are logged into an entry sequenced file, named FTPLOG0. This log is mandatory and cannot be switched off.

The following data is written to the log file. It can be extracted and listed by simple ENFORM queries:

- Event time in MM/DD/YYYY HH:MM'SS format, where
  - MM = Month (01 .. 12)
  - DD = Day (01 .. 31)
  - YYYY = Year (1997 ...9999)
  - HH = Hour (00 .. 23)
  - MM = Minute (00 .. 59)
  - SS = Second (00 .. 59)
- User, requesting the FTP session; this is the user information, presented to FTPSERV-E and it can be the:
  - GUARDIAN ID, or
  - Alias User ID, or
  - Generic user ID
- IP address of requestor
- Fully qualified disk file name
- Event; can be one of:
  - Authentication
  - Close
  - Create
  - OpenRead
  - OpenWrite
  - Purge
  - Rename
- Outcome; can be one of:
  - OK
  - Denied

A simple report may look like this:

```
Event Time          User            Disk File                 Event       Result
---------------  ------------  -------------------------  ------------  ------

08/08/1997 12:28'23  SA.CARL                                Authenticate    OK
08/08/1997 12:29'42  SA.CARL       $GHS1.FTP.GHSCONF        OpenRead        OK
08/08/1997 12:29'43  SA.CARL       $GHS1.FTP.GHSCONF        Close           OK
08/08/1997 12:29'43  SA.CARL       $GHS1.FTP.GHSFILES       OpenRead        OK
08/08/1997 12:29'43  SA.CARL       $GHS1.FTP.GHSFILES       Close           OK
08/08/1997 12:29'43  SA.CARL       $GHS1.FTP.GHSUSERS       OpenRead        OK
08/08/1997 12:29'43  SA.CARL       $GHS1.FTP.GHSUSERS       Close           OK
08/08/1997 12:29'44  SA.CARL       $GHS1.FTP.GHSUSMAP       OpenRead        OK
08/08/1997 12:29'44  SA.CARL       $GHS1.FTP.GHSUSMAP       Close           OK
```

All log file attributes (location, owner, security, size) are configurable in the configuration file FTPEFAST.

If the log file FTPLOG0 does not exist, it is created by FTPSERV-E automatically.

If the log file becomes full, it is renamed, and a new one is created.

Installing FTPSERV-E

The general tasks you must perform to install FTPSERV-E on a system are simply:

1. Configure the FTPSERV-E files according to your needs.
2. Replace the original FTPSERV program with the library enhanced version FTPSERV-E

   - OR -

   Direct the LISTNER process to use the security enhanced FTPSERV process.

The use of dynamic passwords (TimeToken) requires the Authentication Server $AS, which is **not** part of FTPSERV-E.

Escrow Agent

GHS is willing to put all sources into escrow.

Availability

A free, fully functional version of FTPSERV-E is available for a one month trial.

Example Configuration of FTPE-Files

The following sections describe the entries in an example FTPSERV-E configuration and the results for several system users and generic users.

Configuration:

The following tables describe entries are made in the three FTPSERV-E files beginning with “FTPE”:

- System Users (FTPEUSER)
- Generic Users (FTPEUMAP)
- Disk Files (FTPEFILE)

FTPEUSER	
System User	*Access*
GHS.*	
SUPER.TANDEM	
SUPER.SUPER	Deny

All users of group GHS are allowed access

SUPER.TANDEM is allowed access

SUPER.SUPER is denied access

System users who are NOT explicitly mentioned in FTPEUSER are denied access to FTP.

FTPEUMAP		
Generic User	*Password*	*Mapped System User*
Carl	secret	GHS.CARL
$Guest	guest	SUPER.OPERATOR

The generic user ID 'Carl' needs the password 'secret'. FTPSETV runs with GHS.CARL

The generic user ID '$Guest' needs the password 'guest'. FTPSERV runs with SUPER.OPERATOR.

Generic users who are NOT explicitly mentioned in FTPEUMAP, are denied access to FTP.

FTPEFILE		
User	*File Set*	*Access*
GHS.CARL	$GHS1.CARL.*	
GHS.*	$GHS2.GHS*.*	
GHS.*	$GHS2.GHS1.*SRC	Deny
SUPER.TANDEM	$SYSTEM.SYS*.*	
$Guest	$DSV.FTP.FTPSERV	

System user GHS.CARL is allowed access to $GHS1.CARL.*

System users GHS.* are allowed access to $GHS2.GHS*.*

System users GHS.* are denied access to $GHS2.GHS1.*SRC

System user SUPER.TANDEM is allowed access to $SYSTEM.SYS*.*

Generic user '$Guest' is allowed access to file $DSV.FTP.FTPSERV

Any disk files that are NOT explicitly mentioned in FTPEFILE, are not available to any user.

The Resulting User Access:

- Access of System User *SUPER.SUPER*
  SUPER.SUPER can't establish an FTP session; the user is denied FTP access in FTPEUSER.

FTPEUSER	
System User	*Access*
GHS.*	
SUPER.TANDEM	
SUPER.SUPER	Deny

System users not mentioned in FTPEUSER, or having the Deny attribute are denied access to establish a FTP session.

- Access System User *GHS.CARL*
  GHS.CARL is allowed access to FTP; the files he can access are defined in FTPEFILE.

FTPEUSER	
System User	*Access*
GHS.*	
SUPER.TANDEM	
SUPER.SUPER	Deny

FTPEFILE		
User	*File Set*	*Access*
GHS.CARL	$GHS1.CARL.*	
GHS.*	$GHS2.GHS*.*	
GHS.*	$GHS2.GHS1.*SRC	Deny
SUPER.TANDEM	$SYSTEM.SYS*.*	
$Guest	$DSV.FTP.FTPSERV	

GHS.CARL has access to: $GHS1.CARL.* and $GHS2.GHS*.*.

Access to $GHS2.GHS1.*SRC is denied.

- Access of Generic User *Carl*
  The generic user Carl is allowed access to FTP. The non-system password required is: 'secret'.
  Note: The user ID can be configured to be case sensitive but the password IS case sensitive.

FTPEUMAP		
Generic User	*Password*	*Mapped System User*
Carl	secret	GHS.CARL
$Guest	guest	SUPER.OPERATOR

FTPEFILE		
User	*File Set*	*Access*
GHS.CARL	$GHS1.CARL.*	
GHS.*	$GHS2.GHS*.*	
GHS.*	$GHS2.GHS1.*SRC	Deny
SUPER.TANDEM	$SYSTEM.SYS*.*	
$Guest	$DSV.FTP.FTPSERV	

The generic user Carl is mapped to the system user GHS.CARL, and all file access is checked for GHS.CARL

- Access of Generic User *Guest*

  The generic user Guest is allowed to establish a FTP session. The non-system password required is: 'guest'.

  Note: The ID can be configured to be case sensitive but the password IS case sensitive. (The password can be encoded with the utility program FTPWCRYP.)

FTPEUMAP		
Generic User	*Password*	*Mapped System User*
Carl	secret	GHS.CARL
$Guest	guest	SUPER.OPERATOR

FTPEFILE		
User	*File Set*	*Access*
GHS.CARL	$GHS1.CARL.*	
GHS.*	$GHS2.GHS*.*	
GHS.*	$GHS2.GHS1.*SRC	Deny
SUPER.TANDEM	$SYSTEM.SYS*.*	
$Guest	$DSV.FTP.FTPSERV	

The generic user Guest is mapped to SUPER.OPERATOR and all file access is checked for Guest, NOT the underlying system user SUPER.OPERATOR!

FTPSERV-E grants the generic user access to the file $DSV.FTP.FTPSERV.

Overview of the Relations: User to Disk Files

FTPEUSER	
System User	*Access*
GHS.*	
SUPER.TANDEM	
SUPER.SUPER	Deny

FTPEFILE		
User	*File Set*	*Access*
GHS.CARL	$GHS1.CARL.*	
GHS.*	$GHS2.GHS*.*	
GHS.*	$GHS2.GHS1.*SRC	Deny
SUPER.TANDEM	$SYSTEM.SYS*.*	
$Guest	$DSV.FTP.FTPSERV	

FTPEUMAP		
Generic User	*Password*	*Mapped System User*
Carl	secret	GHS.CARL
$Guest	guest	SUPER.OPERATOR

FTPSERV-E is designed, produced, and maintained by

Safe and Secure

*Green*H*ouse* Software and Consulting

Heinrichstraβe 12

D-45711 Datteln/Horneburg

Germany

Phone: +49 (0)2363 72566

Mobile +49(0)172 23 18248

FAX +49 (0)2363 66106

E-Mail Info@GreenHouse.de

Home Page http://www.GreenHouse.de

PGP fingerprint 3A 32 D9 0A D1 25 54 18
11 50 24 84 66 29 2D D2

TANDEM Alliance Partner

In North America contact: Computer Security Products at: Info@TandemSecurity.com

Year 2000 compliance:

FTPSERV-E is Year 2000 compliant.

YEAR 2000 & Beyond