How to Secure Mainframe FTP

Stu Henderson (301) 229-7187
stu@stuhenderson.com
Scott Myers (408) 973-8374
scott@softwareassist.net

AGENDA

I. Introduction

II. How Mainframe FTP is Different

III. Mainframe FTP Security Tools

IV. How To Apply Them

V. Summary and Call to Action

ABSTRACT

FTP (File Transport Protocol) on the mainframe is standard FTP, and talks to every other standard FTP on every platform. However, because mainframe FTP executes on the mainframe, it has several additional capabilities, and several additional security tools readily available. In this session, Stu and Scott explain all this, show you how to secure mainframe FTP, and explain why mainframe FTP is "the most secure FTP you'll find on any platform anywhere".

I INTRODUCTION: FTP (File Transport Protocol)

- **Transfer Files Among Different Types of Computer, Including Windows, UNIX, and z/OS.**
- **Part of TCP/IP (Transmission Control Protocol / Internet Protocol)**
- **Unique Security Capabilities on the Mainframe**
- **We Are NOT Talking About TFTP (Trivial FTP)**

How We Go About This

- **Too Many Options to Cover**
- **Show You Names and Functions; Refer You to the Manuals**
- **You Decide Which Ones You Need; Get Details from Manuals**

II How Mainframe FTP is Different

- **Like Others, Supports *get* and *put* to download and upload files**
- **Transfers Both MVS files and USS (UNIX) Files**
- **In a Syplex, Scope Can Extend to Several CPUs at Once**

Beyond Standard FTP Risks:

- **Access to Both MVS and USS Files**
- **Exposing Userids and Passwords**
- **Access to Printouts**
- **Submission of Batch Jobs**
- **Access to DB2**

Additional Security Tools on the MF

- SAF (System Authorization Facility) to Invoke RACF, ACF2, or TopSecret
- User Identification
- Access Control to MVS and USS Files
- Encryption of Userids, Passwords, Data
- MVS Trusted Computing Base (IBM's Integrity Statement)

Additional Security Tools on the MF

- **Control Over Access to IP Addresses**
  - ***IP is the Routing Part of TCP/IP. Each Computer has an IP Address; IP Routes Messages to and from the Computers***
  - ***Controls Both IP Address of the Mainframe Server and of the Connecting Client Computer***

Additional Security Tools on the MF

- **Control Over Access to Port Numbers**
  - ***At Each IP Address, a Separate Port Number is Assigned to Each TCP Program.***
  - ***When a Message Arrives at a Computer, TCP Hands the Message to the Program Assigned to The Port Number in the Message***

Additional Security Tools on the MF

- **Control Over Access to Port Numbers**
  - ***A Port Number is Assigned to Each Program TCP Can Route a Message to***
  - ***The Program is Called a Daemon, and is a Started Task with a RACF Userid.***
  - ***What Do You Think the Password Is?***
  - ***SAF with SERVAUTH Resource Class Controls Access to Ports***

Additional Security Tools on the MF

- **Control Over Access to FTP Itself**
  - ***The Started Task for the FTP Daemon on the MF is Often Named FTPD.***
  - ***It Often Starts Processes Named FTPD1, FTPD2, …***
  - ***Control Access to All the FTPDx Processes with a Single SAF Rule in the APPL Class (for example, FTPD* in RACF or FTPD- in ACF2)***

Additional Security Tools on the MF

- **Pre-Defined Exit Points**
  - ***An Exit Point is a Place You Can Add an Additional Program (to FTP in this Case) to Alter the Logic of FTP***
  - ***Exit Points Can Be Used to Add Additional Security Checking***

III. Mainframe FTP Security Tools

- **Control File Options**
- **Exits**
- **Security Software (SAF) Rules**
- **Encryption**
- **Policy Agent Software (Firewall-Like Functions)**

Control File Options: TCP/IP and FTP

These Options Can Be Specified in the TCP/IP Control File:

- **IPSEC to specify creation of an IPSEC secure tunnel**
- **NETACCESS to specify a name for a portion of the network to be used with SAF and the security software to control access to the network**

Control File Options: TCP/IP and FTP

These Options Can Be Specified in the TCP/IP Control File:

- **PORT and PORTRANGE along with RESERVED and DENY and SAF to block ports and to give them names to be used with SAF and the security software to control access to specific ports. The keyword UNRSV can be used to specify all unreserved ports.**

- **TCPCONFIG to block the well-known ports**

Control File Options: TCP/IP and FTP

These Options Can Be Specified in the FTP Control File:

- **ANONYMOUS and several related operands (all with names beginning ANON...) which control whether anonymous logons are permitted, and what restrictions are placed on anonymous users**
- **CIPHERSUITE for Encryption**
- **DB2 and DB2PLAN name the DB2 sub-system and plan to be used**

Control File Options: TCP/IP and FTP

These Options Can Be Specified in the FTP Control File:

- **JES2INTERFACELEVEL and several related operands with names beginning JES… for Printouts and Batch Jobs**
- **PORTOFENTRY4 which specifies the POE (Port of Entry) name to be used for this FTP**
- **Several operands with names beginning SECURE_ which specify the level of encryption, whether to use encryption to identify the server, whether to use encryption to identify the client, and similar options**

Exit Points

- **FTCHKCMD which gets control when an FTP command is processed**
- **FTPOSTPR gets control at the completion of certain commands**
- **FTCHKIP gets control at the opening of a new connection**
- **FTCHKPWD gets control when a user types in a new password**
- **FTCHKJES gets control when a user submits a batch job**

Security Software (SAF) Rules:

- **APPL used to control who can log onto a given FTP daemon (you can have two or more FTP daemons running with different characteristics. The name of the rule in the security software is the first seven characters of the name of the FTP daemon started task.)**

Security Software (SAF) Rules:

- **TERMINAL used to control what users are allowed to logon from specified IP addresses. (Used only with IPV4. The name of the rule in the security software is the hexadecimal version of the IP address with the dots removed. Use SERVAUTH resource class in the security software with IPv6.)**
- **SERVAUTH to control access to: the UNIX file system, to given ports, to given IP addresses, to the network itself, to FTP**
- **In RACF the user attribute RESTRICTED**

Security Software (SAF) Examples:

(Using RACF), To Control:

- **Access to FTP:**

```
RDEF SERVAUTH    UACC(NONE)  +
        EZB.FTP.*.*.PORT*
```

- **Access to USS File System Through FTP:**

```
RDEF SERVAUTH UACC(NONE)  +
        EZB.FTP.* * ACCESS.HFS
```

Encryption:

- Encryption is provided in the system software, with a hardware accelerator available.
- Mainframe supports both SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security).
- Also supports Kerberos and IPSEC.

Encryption:

- **All of these protocols can be used to provide encryption of data and encryption of passwords.**
- **Also used to identify the user (instead of the user providing a userid and password).**
- **These protocols can provide protection against sniffer programs (which can read userids and passwords on a Local Area Network).**

Encryption:

- **With SSL or TLS, the encryption keys and digital certificates can be created and managed by means of the security software.**

- **That is, RACF, ACF2, and TopSecret can all act as a certificate authority and provide PKI (Public Key Infrastructure) support.**

Policy Agent:

- **This free mainframe software can provide both Intrusion Detection Service, as well as filtering of messages**
- **For example, filtering based upon: IP address, port number, direction or content**
- **It will not be covered further in this session.**

IV How to Apply The Tools

- **Start by Identifying Threats:**
  - **Unidentified Users**
  - **Improper Access to Data**
  - **Improper Access to Resources, Such as IP Addresses, Ports, FTP Itself**
  - **Unauthorized Browsing of Sensitive Data and/or Passwords**

Then Pick From the Above Listed Security Tools

- For Example, If You Need to Identify Each User, You Might Decide to ID Each User by Means of a Userid and Password
- Then Use Security Software to Control What Files Each User Can Access

Or You Might Decide to Use:

- **Encryption to Protect Both the Data and the Password in Transit**

- **Perhaps TLS or Kerberos or IPSEC or Hardware Encryption)**

Consider Using Tool Combinations:

- **To Let Some Users Access Some Files,**
- **And Allow Other Users to Logon Anonymously and Download One File Containing an Advertising Message,**
- **You Might: (see next slide please)**

You Might:

- **Create Two FTP Daemons with Different Names, Using the APPL Resource Class in SAF to Restrict Users to One FTP or the Other**

- **Use Different Ports for Each FTP and Use SERVAUTH Rules to Control Port Access**

Or Maybe You Want to Have:

- **One Set of Access Permissions for Users Inside the Firewall,**

- **And Different Permissions for Those Outside the Firewall. You Might: (see next slide please)**

You Might:

- **Use the TCP/IP Control File to Assign Different SAF Names to the IP Address Ranges Inside and Outside the Firewall**

- **Use SERVAUTH Rules with Those Names**

And Then:

- **Give Permission to Datasets Based On the Source IP Address**

[for example, in RACF:

PERMIT … WHEN(SERVAUTH(…)) **]**

Start By Protecting All Datasets Completely and Properly,

Then, Based on Your Needs, Select Tools to Control Access to:

- TCP/IP
- IP Addresses
- Ports
- A Given FTP
- USS Files
- Other Resources

Or to Use Encryption

Example A: You want to Let Some Users Download Certain Files,

But Only If They Are Coming From an Address Inside Your Firewall

- **In the TCP/IP Control File Use the NETACCESS operand to group your IP addresses into zones and to give each zone a name.**
- **This name will be used as one component of the name in the security software.**

Example A: You want to Let Some Users Download Certain Files,

But Only If They Are Coming From an Address Inside Your Firewall

For example, suppose that all the addresses 192.168.2.0 to 192.168.2.255 are inside your firewall. You want to put them all into a zone called MYTRUST. You would code in the TCPIP control file:

```
NETACCESS INBOUND OUTBOUND
  192.168.2.0   255.255.255.0     MYTRUST
```

Example A: You want to Let Some Users Download Certain Files,

But Only If They Are Coming From an Address Inside Your Firewall

To create another zone called MYXENO containing the addresses 9.1.1.0 through 9.1.1.255, you would add:

9.1.1.0 255.255.255.0 MYXENO

Example A: You want to Let Some Users Download Certain Files,

Then in RACF for example you would define the two zones in the SERVAUTH resource class:

RDEF SERVAUTH
EZB.NETACCESS.*.TCPIP.MYTRUST
UACC(NONE) …

RDEF SERVAUTH
EZB. NETACCESS.*.TCPIP.MYXENO
UACC(NONE) …

**** Please note that the * in the rule name is a wildcard for the name of the MVS system as specified in &SYSNAME in parmlib***

Example A: You want to Let Some Users Download Certain Files,

Then permit users to access datasets, depending upon the zone:

```
PERMIT EZB. NETACCESS.*.TCPIP.MYTRUST  +
      CLASS(SERVAUTH) ACCESS(READ)
      ID(SOMEUSER)

PERMIT EZB. NETACCESS.*.TCPIP.MYXENO +
      CLASS(SERVAUTH) ACCESS(READ)
      ID(OTHRUSER)

PERMIT 'some dataset name'  ID(*) ACC(READ) +
           WHEN(SERVAUTH(EZB.NETACCESS.*.TCPIP
      .MYTRUST ))
```

Example B: You Are Downloading Confidential Data and Want to Prevent Eavesdropping

- You will need to establish encryption over the link, most likely using SSL or Kerberos.

- In the FTP control file, use the CIPHER_SUITE, KEYRING, SECURE_FTP, SECURE_LOGIN and related operands to set this up for SSL.

Example B: You Are Downloading Confidential Data and Want to Prevent Eavesdropping

- Use the EXTENSIONS AUTH_GSSAPI, SECURE_FTP, SECURE_LOGIN and related operands to set up Kerberos.

- Then co-ordinate their use with the security software administrator (to provide support for digital certificates or passtickets)

Example C: You Want to Let Some Users Download Some Files, Other Users Other Files

- Make sure that the ANON.. operands don't permit anonymous logons. (Or ensure that any anonymous logons are restricted in what they can access. See the details of the various ANON… operands in the IBM manuals.)

- This has the effect of forcing each user to identify himself, using one of: passwords, SSL digital certificate, or Kerberos passticket.

- Passwords will of course be verified by the security software. If passwords are used, make sure that they are encrypted over the network.)

Example C: You Want to Let Some Users Download Some Files, Other Users Other Files

- To set up the encryption, follow the operands in B above.
- Use the dataset protection in the security software to control who can access which files. Optionally, restrict access to the USS (UNIX) file system with a resource rule in the SERVAUTH rule. In RACF you would code:

```
RDEF SERVAUTH EZB.FTP.*.TCPIP.FTPD.ACCESS.HFS
     UACC(NONE)

PERMT EZB. FTP.*.TCPIP.FTPD.ACCESS.HFS
     CLASS(SERVAUTH) ID(UNIXGUYS) ACCESS(READ)
```

Example D: You Can't Rely on Passwords To Prove a User's Identity…

Or You Want to Be Sure Passwords Are Encrypted Over the Network or You Want Protection Against Sniffer Programs

- **To provide all these functions, you would likely use either SSL or Kerberos encryption.**
- **These encryption protocols can serve to prove the identity of the client and/or the server. You would activate them as described in B above.**

Example D: You Can't Rely on Passwords To Prove a User's Identity …

- For SSL (TLS), you would use the SECURE_LOGIN operand to specify client authentication.

- Kerberos always authenticates the client.

Example E: You Want to Let Some Users Browse Others' Printouts

- To allow access to printouts, set the operand FILETYPE JES in the FTP control file, to activate the JES interface.
- You set the value of JESINTERFACELEVEL to 1 or 2.
- The default value is 1 which permits a user to browse printouts and submit batch jobs corresponding to his userid only.
- A value of 2 permits the user to access printouts and to submit batch jobs for other userids, as long as the security software rules permit it.

Example E: You Want to Let Some Users Browse Others' Printouts

You would then use the security software rules in the:

- **JESSPOOL,**
- **JESJOBS, and**
- **SDSF**

Resource classes to control access to printouts and the ability to submit batch jobs.

Example F: Prevent Programmers From Starting FTP Daemons to Harvest Others' Passwords

To do this you will want to block all the ports, and then permit the valid FTP daemon to ports 20 and 20, for example. In the TCP/IP control file, block the ports by coding:

```
TCPCONFIG RESTRICTLOWPORTS
PORT
 20  TCP        SAF     MYPORT20
 21  TCP        SAF     MYPORT21
PORTRANGE 1024-65535   RESERVED
```

(cont'd)

Example F: Prevent Programmers From Starting FTP Daemons to Harvest Others' Passwords

In RACF define the two ports using the names specified in the PORT statements, and permit FTP to them:

```
RDEFINE SERVAUTH
      EZB.PORTACCESS.*.TCPIP.MYPORT20
        UACC(NONE)…

RDEFINE SERVAUTH
      EZB.PORTACCESS.*.TCPIP.MYPORT21
      UACC(NONE)…
```

Example F: Prevent Programmers From Starting FTP Daemons to Harvest Others' Passwords

PERMIT EZB.PORTACCESS.*.TCPIP.MYPORT20
CLASS(SERVAUTH) ID(FTPUSRID) ACCESS(READ)

PERMIT EZB.PORTACCESS.*.TCPIP.MYPORT21
CLASS(SERVAUTH) ID(FTPUSRID) ACCESS(READ)

Alternate Approaches from Third Party Vendors Can Provide Additional Function:

- More Granular Control
- Centralized Logging
- Long Term Archival Logs
- Real-time ID and Escalation of Failed Transmissions
- Integration with Data Center Automation
- Enhanced Cross-Platform Automation

Alternate Approaches from Third Party Vendors Can Provide Additional Function:

- **Support of Regulatory Compliance Through Exception Reporting and Escalation of Security Incidents**

- **Added Functionality to Support Automation of File Transfers (to Compete with ConnectDirect for example)**

V. SUMMARY AND CALL TO ACTION

- **You Should Understand Now Why We Say That This is the Most Secure FTP Commonly Available Anywhere, Because of:**
  - **Tools from IBM and Computer Associates**
  - **Security Provided by MVS Platform**
  - **Control File Options**

For Further Information:

- See articles and back issues of the RACF User News and Mainframe Audit News at www.stuhenderson.com
- IBM manual “z/OS Communications Server: IP Configuration Reference”, SC31-8776
- IBM manual “z/OS Communications Server: IP Configuration Guide”, SC31-8775
- Computer Associates Cookbooks for ACF2 and TopSecret

End of Presentation

Thanks for Your Kind Attention.