JDEtips Journal September/October 2006 Volume VII Issue 5

Keeping Your i5/OS Users Out of Mischief

By Glenn Robinson

Editor's Note: *You can't be too safe when it comes to operating system lock downs. Yet so few companies go beyond user roles and Object Authority to secure their systems. Glenn Robinson tackles this all-too-important topic with regard to i5/OS. So read on for how to protect your data from unauthorized access and save the office mischief for less dastardly deeds (like putting the office coffee pot back on the burner empty).*

You may be thinking, "Not another article on security!", but read on anyway. I have read many really good articles on how to implement solid security on i5/OS and its predecessor OS/400, which go beyond the standard Object Authority. And yet, I don't see this implemented in too many places.

Now, there's no doubt that having effective user profile, password management policies and controls is an absolute necessity; it's like having a decent lock on your front door with latches and dead locks too. But it is by no means where we should stop.

User profile and password management is not exclusive to i5/OS, but rather a necessity for all commercial operating systems. The difference with i5/OS is that security is built into the operating system and also built into the low level microcode, the System Licensed Internal Code (SLIC).

In the last decade, i5/OS and OS/400 have changed dramatically to react to the changes in technology and end user requirements. I remember all too well the Windows and Unix people laughing at the AS/400 and telling us it wasn't "Open" and was a legacy system; how wrong they were. Because IBM responded so well with the iSeries and AS/400, we now have an absolute plethora of ways to access the system and for i5/OS to access other computer systems. It's fortunate that every time IBM has opened up access to the system, they've also been extremely diligent in ensuring that security of the system has remained paramount.

It's no good just putting good locks on your front door any more; you need locks and bars on the windows, too (pun intended).

The Five Security Levels

i5/OS has five security levels built in, which we call levels 10, 20, 30, 40, and 50.

It's no good just putting good locks on your front door any more; you need locks and bars on the windows, too (pun intended).

Level 10 security, which is no longer available on i5/OS, required the user to enter a User ID, but no password was required. You can see why IBM disabled this level a number of years ago.

Level 20 requires the user to enter a User ID and a password. Once the user has entered the correct credentials, they then have access to the entire system.

Level 30 is what we refer to as Resource Level Security. As with level 20, the user must enter valid credentials, but once logged on, the user is only authorized to access the files, programs, and other objects to which they have been granted authority.

Level 40 is called Operating System Integrity Security. This security level implements the functions included in level 30, but also restricts user-created programs from executing certain low level functions. Low level functions are now only available via published IBM-supplied APIs, of which there are many hundreds available.

Level 50 enhances Operating System integrity even further and is implemented in i5/OS to permit customers to achieve FIPS-140, C2, and Common Criteria certifications.

Which level should you use? New System i5 servers with i5/OS partitions will default to security level 40 because this is sufficient for the majority of customers. There are certain situations where a customer will choose level 50, but that's unusual. A number of customers remain at security levels 20 or 30; my advice is that they really should very seriously

consider a move to level 40. I believe that IBM should also disable level 20 because this does leave the system open to abuse once you are logged on to the system.

The average 'green screen' user is quite easily managed and controlled, but the more complex security implementations occur when user access to the system is via a method other than 5250 terminals. This is where IBM has really got cute over the last decade in enhancing and reinforcing the security of i5/OS in terms of protecting the entire operating system and user object environment on the system from the varying access methods available to the user now.

Registration Information

Hopefully most of you will have heard of Exit Points under i5/OS. These are specific points in IBM, and third party applications, where you can attach your own code. There's an exit point for the Power Down System (PWRDWNSYS) command, QIBM_QWC_PWRDWNSYS. If you register your own CL/RPG/COBOL/C/C++ program against this exit point, it will get called whenever anyone executes the PWRDWNSYS or ENDSYS command. The program can be whatever you want.

Just as useful are exit points that can be used to call your programs when:

- a user logs on to the FTP Server
- an authorized FTP user attempts to run an FTP command
- a user accesses the database via ODBC/JDBC
- a User Profile is created/changed/deleted

These are always the easiest programs to code, but there is plenty of example code out on the Internet. The System i5 Information Center has example exit point programs that can help you get started.

If you want to see a full list of Exit Points, run the WRKREGINF command from a 5250 command line. Option 5 against any exit point shows you all the associated details, but option 8 is where you add/remove the programs you want to work with for a particular exit.

Figure 1 illustrates that Exit Point QIBM_QSY_DLT_PROFILE has three exit programs associated with it; these will be executed in ascending numerical sequence.

Function Identifiers

We may not want or need to add our own programs to enhance the security, but we may—and probably will, want to enhance the security of some of the less traditional functions now available on the system.

Function Identifiers tags relate to application functions such as:

- iSeries Navigator functions
- Use of Data Transfer
- Access to the system via PC5250
- Use of IBM Director functions
- Control over FTP Server and Client
- Access to Job Logs of *ALLOBJ users
- Use and Administration of IBM Director

Let's say you are concerned about FTP usage (you should be), and you'd like to ensure that only certain User Profiles can access the system using FTP. We can control this, without having to worry about exit point programs, by editing the Function Identifier entry for FTP Logon Server, QIBM_QTMF_SERVER_REQ_0. To access this, you can execute the Work with Function Usage (WRKFCNUSG) command at the 5250 command line or use Application Administration from iSeries Navigator.

```
                          Work with Exit Programs

Exit point:   QIBM_QSY_DLT_PROFILE     Format:   DLTP0100

Type options, press Enter.
  1=Add   4=Remove   5=Display   10=Replace

              Exit
            Program      Exit
Opt          Number      Program        Library

               5555      QYPSUSRPEX     QSYS
           27694187      QHXHDLTU       QIWA2
         2147483647      QGLDPUEXIT     QSYS

                                                                  Bottom
Command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F12=Cancel
```

Figure 1 – Work with Exit Programs