ARTICLE

Is The Door To Your Company's Private Data Wide Open?

By Robin Tatam

When I began my career on the AS/400® more years ago than I care to reveal, life was simple—"dumb terminals" ruled the computing kingdom and subfile displays were considered cutting edge. Application menus blocked users from direct database access and security-conscious administrators could set up a profile to limit user capabilities to a few basic commands.

Then, things got complicated. First, everyone flocked to *programmable workstations*, better known as PCs. As a result, business software, including spreadsheet applications, developed rapidly. And, because core line-of-business applications were still running on the AS/400, file transfers between PCs and servers became common.

Pandora's Box

IBM responded to the new market demands for open database access by building TCP connectivity into the AS/400 (now re-branded as the iSeries®). In addition to the traditional 5250-based "green screen" applications, the iSeries could now be accessed through File Transfer Protocol (FTP), Open Database Connectivity (ODBC), Distributed Data Management (DDM), and other interfaces. No one thought much about the security ramifications, but it was like opening Pandora's Box!

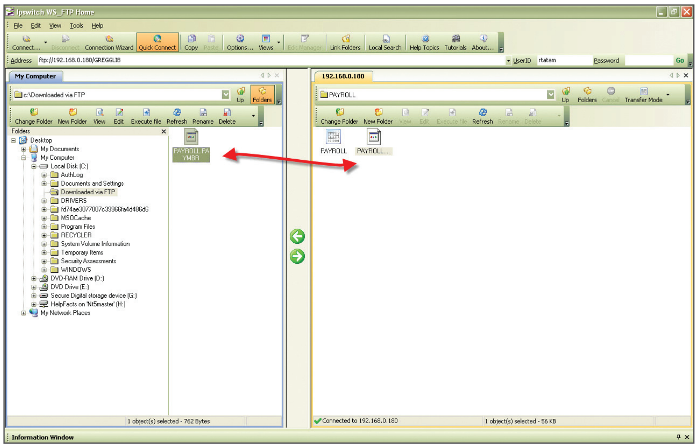
Fast forward through a few server name changes to the current day...

Because all of these interfaces connect directly to the server's database, the menus that historically restricted green screen users are no longer effective. The "secure menu" has become a thing of the past; now, we must rely on resource (object) security to protect data. Object security, an integral part of the operating system, is rock solid and works with every interface that today's IBM Power Systems™ support. Yet, as the PowerTech annual State of System i Security study reports every year, object security is rarely fully implemented and is easily circumvented by powerful user profiles. That's why most industry studies of lost, stolen, or corrupt data, point to internal corporate users as the culprit.

Object security is recommended for the core layer of protection. Unfortunately it is a "one-size-fits-all" approach because it does not distinguish between different user interfaces. If you implement the best practice recommendation of "deny by default" for green screen access, you really can't use legitimate PC tools to access the data. For example, a user with change-level access to data with a menu-controlled green screen application will have that same access with powerful SQL-based applications such as FTP and DDM.

FREE: Unauthorized Access to Sensitive Data for 30 Days!

Don't think a user could take advantage of those authorities? Think again. A PC-based FTP program, such as the one shown in Figure 1, provides full graphical access to any authorized or unsecured library or IFS directory. This application costs less than $40 and comes with a free 30-day trial!



Address ftp://192.168.0.180/GREGGLIB

UserID rtatam

Password

c:\Downloaded via FTP

PAYROLL

1 object(s) selected - 762 Bytes

Connected to 192.168.0.180

1 object(s) selected - 56 KB

Figure 1. Authorized Drag-and-Drop Access to Sensitive Data

To make matters worse, several of these network interfaces let users submit and execute host commands, as well as run commands and edit database files. Object security is still in effect for the command and any objects that the command uses. But, it is important to understand that a user profile's "limited capabilities" setting (used to restrict command line functionality) may not be honored outside of the green screen. For example, depending on the specific operating system level, the FTP server either honors the setting or ignores it.

Finally, network requests are not logged or audited by the operating system. More and more customers are auditing user and system events with QAUD*xxx* system values. But, these values don't monitor network activities—the most you can learn is *when* a file is opened, not *what request was made* of its data.

A Hodgepodge of Options

Because of the clear danger of unwanted system access through network interfaces, can you still use these interfaces for legitimate business reasons? And if so, how do you control them? Several methods are available to help secure these interfaces, each with its own pros and cons:

- You can prevent some services from starting by using the *GO TCPADM* command menu or Navigator for i (formerly known as iSeries Navigator). Verifying that someone does not restart the services, or forgets to shut them down after using them temporarily, are issues. Plus, server requests are not visible for reports or alerts. And, you are dependent on the underlying object security model.
- You can use the IBM i commands plus the *Application Administration* portion of Navigator for i to select which functions individual users control. This allows you to override some settings normally restricted by operating system security. On the downside, it offers no visibility, no alert mechanism, and no reporting. Plus, not all services are covered by functions.
- You can define exit programs for most network interfaces. You use the Work With Registration Information (WRKREGINF) command to define the name and location of an exit program for each service. (An exit program, similar to database trigger program, is called by the associated exit point when the server receives a request. The exit program receiving details

about the incoming request should determine the legitimacy of the request and log the activity.)

Exit programs *are not* synonymous with security—the functions performed by an exit program are defined by the programmer who created it. Some exit points allow exit programs to approve or deny requests; others simply perform a programmed function. For example, the "create user profile" exit point might call a program to create a work library for a new user. While it is possible to write your own exit programs, many organizations don't want the cost and effort of developing and maintaining complex, security-sensitive applications with potential performance implications.

The Professional Solution

If, like most organizations, you decide to use a professional network security solution, we recommend PowerTech Network Security. As the leader in security solutions, PowerTech makes all of the necessary functionality available as a standalone solution, or as part of the PowerTech Compliance Suite—a collection of several popular solutions for securing Power Systems running IBM i.

When you install and activate Network Security, network requests to the server are visible instantly. The information is stored in a secure IBM repository for analysis and reporting (see Figure 2). For user and application requests that involve server access, including remote commands, you can issue alerts for immediate notification and response.

Imagine being able to report on a user accessing your Integrated File System (IFS), including the directories navigated and the files viewed or deleted. How reassuring to know that if an FTP user attempts to target a secured production file, the unauthorized access attempt is blocked and the system administrator is notified automatically!

Network Security also offers the ability to have a request run under an alternate profile. You can implement "deny by default" methodology while granting temporary access to pre-approved requests. For example, you could set authorities on a library to *EXCLUDE, but still allow a specific file to be downloaded and logged by your accounting group.

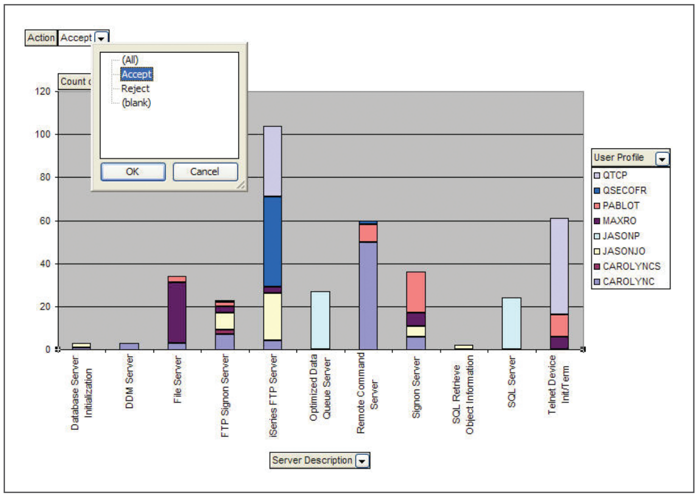
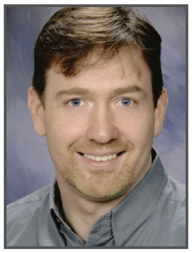


Figure 2. Analyze, Control, and Report on a User's Network Activities

Or, you could take an unrestricted user profile with *ALLOBJ special authority and downgrade it to read-only capabilities for production data. Both of these "on-the-fly" security changes are transparent to the user and remain in effect only during specific requests.

For more information on **PowerTech Network Security**, or to receive a FREE compliance scan of your system (including a review of your network vulnerability), visit the PowerTech Web site at www.powertech.com.



Robin Tatam *is the Director of Security Technologies for PowerTech, a leading provider of security solutions for the System i.® A frequent speaker on security topics, he is co-author of the IBM RedBook,* System i Security—Protecting i5/OS Data with Encryption. *Robin can be reached at:* ***robin.tatam@powertech.com****.*