PowerTech
your security expert

ARTICLE

IBM Eye: Security Detective for Hire

By Robin Tatam

Fifty years ago this fall, long before my time, a brand new TV show called *Hawaiian Eye* premiered. It featured its own cool theme plus a detective agency/private security firm that specialized in security services and protecting clients. Since then, the world has watched private detectives help their clients get and stay secure for half a century. Today, I think of myself as a modern IBM Eye, a private detective with my own cool theme: I remove security threats to Power Systems™ running IBM i (System i,® AS/400®) for my clients.

As I've worked with clients, I've found that many people don't know if they need security for their Power Systems servers. Or, they don't know how to go about securing them. So, I wrote this article with two purposes in mind: 1) as a "wake-up call" for the customers who think that "powering the server on" is all the security they need, and 2) to help organizations that are struggling to get started with security. It's a step-by-step overview of how to deal with some of the most pervasive security threats currently facing IBM Power Systems.

Step 1: See Where You Stand

Of course you have a vested interest in ensuring that your server is secure, but where do you begin? Many clients who use my services are confused about trying to compare the different metrics of protection with their most important and fragile technology asset: corporate data. One of the best sources of information for IBM i security controls is the annual *State of System i Security* study published by PowerTech, a leading provider of security solutions for IBM i. Compiled from data collected anonymously from assorted systems, the 2009 edition of the study is available free as a download from www.powertech.com. If you are interested in seeing how other systems measured up against industry "best practices," it's a very valuable read.

A good first step is to see how your *own* server measures up to these standards. It's difficult to secure any system, especially when you don't have a plan. I am often hired by organizations that are trying to fix things without having a basic understanding of the issues.

The PowerTech Group, Inc.
www.powertech.com
TEL USA: 253.872.7788
TOLL FREE: 800.915.7700

Many have simply inherited their configuration. What surprises many of them is how easy and inexpensive a basic compliance review is. I have performed dozens of free assessments for customers using PowerTech's automated Compliance Assessment tool. *They* like it because it provides real-time results without any "heavy lifting" on their part; *I* like it because it allows me to focus on advising them how to interpret their assessment information.

I recommend that you perform a free assessment to decide whether a more detailed review—a "deep assessment"—is justified. Once you complete an assessment, you compare the findings to standards. If you do not currently have standards, a number of "best practices" are available for IBM security metrics such as user profiles, system values, and object authorities.

Step 2: Create Your Security Policy

A security policy is a top priority. If you don't have one, your strategic team should develop a policy that is not technology-specific. And, someone more senior than an Information Technology (IT) administrator should make policy decisions. (There always should be input from IT, but keep it in perspective—the system administrator often has too much responsibility in this area.) If you do not know how to create a security policy, check the *open source* security policy, available through PowerTech at www.powertech.com, as a starting point. Regardless of the source, it is important that policy components, such as reasonable usage and password policies, are communicated to your user community. Share the policy on a recurring basis to keep it fresh in everyone's minds.

Step 3: Learn Your System's Arsenal

You can perform most of the work of securing your Power Systems servers using tools the operating system provides. Commercial tools can *reduce* exposure in poorly secured systems, but there is always a requirement for the operating system (IBM i) to prevent an access "free-for-all." Becoming familiar with IBM i controls is necessary to build an infrastructure that is secure regardless of the user interface. Many software vendors rely on code and menus for security, rather than implementing resource (object) security. And, many commercial applications use your existing security configuration. Others adopt dubious practices, such as requiring users to have *ALLOBJ special authority, to ease their support burden. Inexcusable!

Commercial security solutions complement IBM i functionality. These solutions offer a number of benefits: audit independence, advanced functionality, support of operating system changes, ongoing development, and reduced staffing needs. For example, I help clients by using PowerTech's set of commercial solutions designed for compliance, capturing security events, and fast problem notification.

Step 4: Lock and Load Security Values

For server properties, IBM i uses a mechanism called *system values*. Each system value belongs to a category; security values belonging to the *SEC category. You work with security values using the *WRKSYSVAL *SEC* command. Arguably the most important value is QSECURITY, which indicates the overall server security level. I say "arguably" because organizations often have so many other things configured incorrectly that this value isn't relevant. For example, if you are running your server at the highest security level (50), but providing each user *ALLOBJ authority, in reality you are running at security level 20. I see similar issues in virtually every compliance review that I do.

To start, print a list of your system security values and understand them. (IBM's security manual provides detailed information, and there are numerous online tips and techniques, including PowerTech's Compliance Guide.) It is important to use these values to enforce business policies. Don't change your values without careful consideration. Some values require an IPL to initiate or undo. Others, such as the Password Level system value (QPWDLVL), are even more difficult to undo.

The IBM operating system version 6.1 offers several new security system values for password management and Secured Socket Layers (SSL). (See the *System i Security Reference Version 6 Release 1 [SC41-5302-10]* for more information.)

Step 5: Set Up Good Roadblocks

A Security Officer specifies individual capabilities through user profiles. A user profile/password combination is the main barrier that guards valuable data and applications. The PowerTech security study shows that far too many users have overly powerful special authority capabilities combined with weak passwords (for example, a password that matches the profile name).

- Consider creating passwords with a random value and requiring new users to request to sign on for the first time. This reduces exposure when a new user is hired. And, do not rely on the "set password to expired" control because anyone can gain access *first* and *then* assign a new password.
- Once housekeeping is complete, use policy and business processes to prevent an issue from recurring. Group profiles provide advantages such as groups owning newly created objects instead of individuals. Assigning groups significantly reduces administration of object security by addressing members as a single entity. Additions to, or departures from, the team impact only the group membership, not the numerous object authorities. For example, if you ever have to delete a user profile, you'll appreciate group profiles.
- Treat the special authorities associated with a profile as special. In the assessments that I conduct, users often are assigned authorities completely unrelated to their job function. Of the eight special authorities, *All Object (*ALLOBJ)* is the most dangerous. This gives users unrestricted access to every program, every data file, and most server functions! Combined with command line access, it provides them the ability to obtain any of the other seven special authorities and run jobs masquerading as other users. A user inherits any special authorities granted to their group profiles. So, *do not* give special authorities to end users.

  For special functions such as starting a printer or resetting a password, use a profile-switching solution such as PowerTech's Authority Broker.
- Use profile templates, instead of copying a "similar" user profile, to reduce the chance that specific modifications ripple through the user community. Otherwise, the most-recent profile might be totally different than the original.

To sum it up, create user profiles based on job role (or application use), use group profiles, and audit your profile attributes to ensure that they conform to your security policy. For special authority profiles, or private data authorities with command line capabilities, use the operating system's profile auditing functionality.

Step 6: Stop Quick Getaways

Considering the number of articles and educational events explaining the risk of network-connected PCs, it's amazing how often I see servers with little or no network protection. The *2009 State of System i Security* survey indicates that 65% of the servers surveyed fall into this category.

Security is often a combination of command line restrictions and application controls. TCP services, such as FTP and ODBC, opened corporate data to powerful desktop applications and supplied users with a direct database connection that avoids these security controls. All interfaces must follow the operating system's resource security rules. But, there are significant issues if you use the operating system as the *only* control for both green screen and network interfaces:

- Few shops have implemented object security correctly—they usually rely on an outdated security model.
- Object security is a "one-size-fits-all" setting that does not distinguish between interfaces.
- Many network transactions, such as file transfers, are not audited
- Some network interfaces provide command line functionality that ignores the user profile's "limit capabilities" restriction.

These interfaces often have exit points that allow you to designate an exit program that gains control before execution of the request. These user-written programs can reject or approve a request. With over 30 exit points related to network transactions, it is important that user requests be audited and controlled. You can write basic exit programs from online examples. A more sophisticated commercial solution should integrate seamlessly with operating system upgrades, while ensuring that exit programs don't impact your business processes. I recommend Network Security from PowerTech.

Step 7: Put Everything To The Test

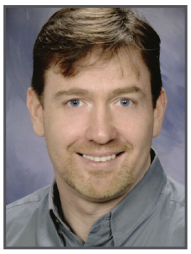
You must plan your new security infrastructure carefully. Break the implementation into measurable phases, whose success can be gauged—good security can't be rushed. You should test your changes ahead of time and keep a detailed log of changes as well as an "escape plan". Create test profiles to ensure that critical business functions will continue to work after a change is implemented.

Take advantage of the operating system's ability to audit authority failures, object creation and deletion, and security events. It can provide information during testing, deployment, and compliance monitoring. Enable the audit controls included in the operating system by using the *CHGSECAUD* command (V5R3 or later). Be sure that your security and compliance deployment game plan considers the impact of all changes and exposures. Use a centralized solution, such as PowerTech's Compliance Monitor, to review audit information.

For reference, the IBM security manual and Redbooks are available online. The book, *IBM i & i5/OS Security & Compliance: A Practical Guide*, is also available from various online retailers. It contains details about the controls available in the operating system through level 6.1. For a list of other IBM resources, search online for "OS400 security," "i5OS security," or "IBM i security."

Step 8: Keep An "Eye" On The Future

Security and compliance is a journey, and a good security policy is the blueprint you use to measure your progress. You don't simply set up your environment—you must use the tools IBM provides to audit and control user activities. You need defined procedures to review log entries and a commercial solution to perform the "leg work." After you complete these basic recommendations, your future phases should include Secure Socket Layers (SSL) for client connections, encryption, and advanced intrusion detection. Threats to your organization and your corporate data are always evolving—your security must be ready.



Robin Tatam *is the Director of Security Technologies at PowerTech, the leading provider of security solutions and services for Power Systems running IBM i. He has been a consultant for 20 years in the U.K. and the United States. He regularly conducts training around the country, including COMMON. Robin provides critical vulnerability assessments and other security services. He can be reached at:* ***robin.tatam@powertech.com****.*