Communicating With Sam

Privacy and Governance: Adapting iSeries Security

Sam Johnston

Question:

Our management is becoming increasingly concerned about security of our company data from misuse by internal resources and our compliance with corporate and government regulations. They feel that our iSeries may not have or be capable of the appropriate level of security to ensure the privacy of confidential data. Our current security method is built around menu option limitations that functioned very well since the days of fixed function terminals. What is the best method to minimize access to a file, for the user profiles that have *ALLOBJ authority? How do we get started on upgrading security?

Answer:

Organizations spend a significant amount of resource effort in protecting themselves from hackers that may want to access confidential data through the Internet. While these security risks are real, you have pinpointed what is potentially a greater threat – employees, some of which inadvertently gain access to trusted information, or worse rogue employees that take advantage of trusted relationships to access company data. The security danger associated with employee breaches is magnified by the fact that, unlike outsiders, employees have insider knowledge that enables them to rapidly hone in on key information.

Ultimately, organizations need to protect production business data on the OS/400(i5/OS) properly by using the correct security methods that IBM have provided in the operating system. OS/400 (i5/OS) provides the tools to create what is referred to as the "least privilege" security model and this needs to be implemented into the production environment. Menu driver security when objects have all object authority will not meet the compliance standards in today's business environment.

External auditors are becoming much more critical on this issue as a result of their efforts becoming increasingly dependent on thoroughly performed IT audits. Shareholders, and agencies that protect their interests, are holding corporations to a higher standard when it comes to the integrity of financial information that is produced by ERP systems. Your security efforts need to evolve and respond to these changes

Before we have an external auditor knocking on our door we had better address this legacy security issue on the production data and solve it with the "least privilege" industry standard. Microsoft, Linux and AIX use this standard as well. Imagine the repercussions if an external auditor logs on to your OS/400 (i5/OS) and uses FTP, JDBC, ODBC, DDM, DRDA, OLE DB, ADO/OLE DB or some other newly created technology to access data and downloads, deletes and/or modifies the payroll file or accesses an output queue that shows them social insurance or credit card numbers of clients or employees.

The theory of Network Administrators controlling ports for data access is a good one for controlling access, but once access is obtained; the security protection is based on the controls on the object container and data object itself. Network Administrators control access to the system; and NOT access to the object once access to the system has been approved. Therefore, if the Network Administrator allows access for a trusted third party or a contract employee, that person may have access to privileged information that could severely impact your business. This access risk needs to be eliminated by security controlling authorized users from a system level and restricting them to 'must have' information.

A number of people have "quick fix answers" to solve the issue but the only real business solution for OS/400 (i5OS) is to get your system to object level security.

eServer i5 595
Designed for medium to large enterprises, the model 595 is the largest server in the eServer iSeries family. It offers multiplatform management and maximum flexibility for customers requiring up to 64-way symmetrical multiprocessing capability.

Many organizations resist making this change due to the view that it will take forever to get all of your production objects to the "least privilege" security needed to meet compliance. While it will take a considerable amount of time and effort, delaying the decision to get started will only increase the challenge and risk. The decision is complicated by the fact that most production OS/400(i5/OS) environments have taken a very long time to evolve to the state they are in today and most are managed without the large staff of people it takes to manage other environments. One of the first decisions should be to assess whether you have the internal skills and resources to complete this task in house or should you bring in outside assistance. Once this project is complete and new processes, policies and controls are in place, the management of these processes on the OS/400 (i5/OS) can be done with minimal time and effort by your staff, but without the right resources you will never get to the maintenance state.

Now that we know we should implement the industry standard of "least privileged" in the OS/400 (i5/OS) environment, how do we do it?

In order to get to this new world model of security you must remove the *ALL OBJECT authority from all production business objects. By clear definition "ALL" means everyone, everything and everywhere on your system. Achieving the goal will require a detailed project plan just like most other IT projects. At a high level, you will need to divide the project into a few key phases.

Phase 1 - Gaining Commitment and Control

1. If your company has a Chief Security Officer then you have a champion to sponsor a project like this. Gaining the support of key stakeholders and other senior executives is going to be a major factor in the success of the project. Security is everyone's issue; make sure you involve the areas outside IT in the process.
2. Incorporate the new security model into the change management process to ensure that the development and production teams don't inadvertently undo your security with other projects and changes.

Phase 2 - Information Gathering and Design

1. Review any production objects that are owned by QDFTOWN and assign the correct owner. (OS/400 available commands and programs automate this process).
2. Review the public authority of each production object and all explicit authority to production objects. (OS/400 available commands and programs automate this process).
3. Review the production programs on the system to see the authority required to run the program. (OS/400 available commands and programs automate this process).
4. Review the production system job descriptions to see library lists and authority. (OS/400 available commands and programs automate this process).
5. Obtain a list from your Network administrator of all User profiles that have access to ports on the OS/400 (I5/OS) system through the network for the purpose of accessing data. These are the first User profiles you need to be concerned about.
6. Gain approval to apply audit functions to any User profile that can promote to the production system or remove data from the production OS/400 (i5/OS). Remember adding Audit functions may impact system performance so people need to

be aware of this; but adding audit functions are needed to ensure compliance.

7. Identify Production objects and then categorize each object by level of security needed. For example, Classified, Non – Classified, Top Secret, etc…
8. Identify production data Owners by business function. For example, accounting, receiver, shipping, inventory etc…
9. Review the personnel job descriptions with the department manager to determine if employees perform functions outside of their job descriptions. (These functions need to be known before changing security on objects).
10. Map all system users in your organization to production applications and data required to complete their business function.

Phase 3 - Deployment / Testing

1. Apply audit functions to the required User profiles.
2. Divide your categorized data by business function application and implement NEW Group Profiles for each application. As a rule Group Profiles should not own objects.
3. Add the new group profile to each required production object. (OS/400 available commands and programs automate this process).
4. Request one persons User profile from the department head that you can change and test changes made. This way you are assured this person can perform all required business functions. Once the testing is complete and the department head signs off; obtain a list from the department head of all User profiles that perform the same task and then make the required changes for the rest of the people the perform the same function.
5. Once all User profiles are attached to the correct new group profiles you can change the old group profiles to not have a password and start removing the old group files from your OS/400 system after they no longer are the owner of objects.
6. You may need to add a few special explicit authorities to a few User profiles to allow for certain functions to be performed for cross application Users.

Having gone through this process, it is essential that you monitor and maintain the security model. A regular external audit is required to ensure the new standards are still in effect. This doesn't have to be a manual process by expensive external audit companies. For example, Skyview's Risk Assessor is an inexpensive application you can use to compare your security configuration to best practices as noted in the OS/400 Security Reference manual. The application produces a complete independent analysis that would normally take days to produce through other methods. By automating the audit function and third party expert review you can focus your resources on improving your security based on the outcomes of the automated review.

These steps will help you get started on the "least privileged" industry standard security design. Just remember that security is about creating layers and always staying one step ahead. While adopting the "least privileged" model is a good start, resist the temptation to remain static. Up the ante and advance your iSeries security to the next level. Once you have the object level security implemented, investigate the more advanced record (field) level security on objects to add depth and layers to your security model. TUG

Sam Johnston *is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com.*
Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday June 10, 2005.