Securing the Change

By Mike Struyf

The Challenge

Change control systems must allow users to be designated with certain rights to manage your applications. These rights allow change control events to be performed by users with specified capabilities, while at the same time not allowing that user to perform the same events outside of change control.

For example, a specific user may be granted rights to perform promotions into production libraries. It is critical that promotion actions be done only under change control while not allowing the user to update the production libraries manually outside the control of a change management system.

A typical IBM i security scheme would be one that would allow the user that has promotion rights to also (undesirably) be able to directly change the production library. For example, the person that can promote to production could manually delete a program from that production library outside of change control.

What is really needed in this case, is the ability for the user to perform change control tasks within the confines of the change management system while at the same time preventing that same user from having authority to directly update the libraries outside of the system by providing the user with unnecessary privilege escalation.

The IBM i operating system has a feature, that when used appropriately, meets this need with flying colors. This feature is known as program adoption. Program adoption on the IBM i allows a program while running, to "adopt" the authority of a different user profile. This is typically used to have a program run with more rights than the user actually has.

This feature, while providing flexible functionality can also present security risks if implemented improperly. Two key security exposures are common when using adopted authorities. With the correct technique these exposures can be eliminated.

The first potential exposure occurs when a program that "adopts" makes unqualified calls to other programs or commands. By using unqualified calls, the user can manipulate the library list and cause an illegitimate program of the same name (but in a library other than expected) to be called. This illegitimate program would still be using the adopted authority of the original calling program and could result in a variety of security problems, such as allowing the user a command line that adopts QSECOFR rights; a very serious security violation.

The second security exposure is in allowing the adopting program itself to be called directly. In this case, any unknown caller could call the QSECOFR adopting program directly and gain elevated security access.

The Implementer Advantage

Any reliable change management system must at its core allow for customized user capabilities, while also allowing for the protection of product library integrity outside of the change management system itself. And in doing so, there must be no possible compromises to system security.

PTC's Implementer's Secured Promotion Technology (SPT) takes advantage of adoption to provide a secure and highly auditable change control environment while avoiding any potential security exposures.

Implementer avoids these problems by ensuring all QSECOFR adopting programs have no unqualified calls or commands, and by using a dynamic security token to prevent its QSECOFR adopting programs from being called directly by unknown callers. The security scheme includes a handshake with the calling program to ensure it is being called from a known legitimate caller. If this handshake fails, not only is the action not allowed but a message is also sent to system administrators to indicate a potential attempted

security breach. This approach ensures only valid Implementer functions are using the QSECOFR adopting programs.

Tools and user written programs not using these techniques have the following potential problems:

- If not using adoption at all, too much authority must be given to users to perform their job. This results in security and audit breaches.
- Adoption schemes without the features mentioned above could result in larger problems than they solve, such as serious security breaches.
- Adopting programs that have unqualified calls often will fail an audit.

Summary

To best protect your software assets, your change control solution needs to ensure that key change control events can only occur under change control and that those same actions cannot be done manually.

Implementer's proprietary Secured Promotion Technology (SPT) provides just such a solution. For more information about the Implementer product, please visit PTC's Implementer product page at: https://www.ptc.com/products/implementer

About the Author

Mike Struyf is a Principal Software Development Engineer at PTC for the Implementer change management system. An employee of PTC since 2011, he has been helping manage code change in IBM i applications for over 22 years since graduating from Benedictine University in Lisle, IL in 1997.