SKYVIEW
PARTNERS, INC

Object Level Security vs. Exit Point Security

by Carol Woodbury

The question regarding exit points is something we at SkyView partners have been explaining and discussing with various prospects and customers during the 5+ years that SkyView Partners Inc. has been in existence. The issue is that of Exit Points vs. Object Level Security.

An interesting twist in this age old dilemma is the fact that some Exit Point vendors have taken to claiming that their solutions implement or are “object level security” which is truly an odd premise to assert. The reality of the situation is that object level security is built into i5/OS as the default security mechanism. While the system is not “locked down” when you unpack it out of the box, object level security is a feature that is there, from the first time the system is IPLed. It’s up to every individual organization as to how tightly to control access to the objects – in other words, what object security settings to use. The alternative to object level security is to deploy an exit point security scheme which, in our opinion, is fraught with weaknesses.

Before I cover the weaknesses of securing your system with Exit Points, keep in mind that object level security “reigns supreme”. In other words, it is the object’s (file’s, library’s or folder’s) security configuration that ultimately allows or denies access to the data. Now let’s look at some issues with exit points.

1) **Exit Points don’t cover all the ways you can access data.** Currently there are no exit points for the HTTP server, Sockets or anyone on your system that already has or can get command line access. So you can lock a lot of the doors and windows, but gaping holes remain. This is not the case with object level security. Once you have a solid object level security scheme in place, REGARDLESS, of the method used to access the object, object level security is in effect.

2) **Exit Points require you to leave the actual object at an access control setting of something other than *EXCLUDE if anyone is to gain access via that network interface (e.g., ftp, ODBC, DDM or SQL).** Best practices require that sensitive or private data be placed in files where their default access is set to *EXCLUDE, meaning that no one can just log in and view, change or delete data. Best practices cannot be attained if the object is set to something that is greater than *EXCLUDE. In the case of exit points, exit points are the “access granting” mechanism that determines who gets access; therefore, the underlying objects’ default (*PUBLIC) acceess cannot be set to *EXCLUDE if some users must get access through exit points. Therefore, instead of the object, the exit point attempts to be the “gatekeeper” to the data. If the user passes the exit point tests, the exit point says “OK, you can have access”… And the user has access to the data… This is probably an OK way of doing things, except that:

   a. Exit Points don’t cover all the ways to get at data. So objects that are set to something other than *EXCLUDE are available to the HTTP server, Sockets and command line access. People can use these methods to gain access to data and will remain undetected by the exit point. This undetected access wouldn’t – rather couldn’t – that is, i5/OS doesn’t allow it to - happen with a good object level security scheme in place

   b. Since you have to leave object in an “open” state (Open = something other than *EXCLUDE) you cannot claim that your data access methodology is “deny by default”… Deny by Default is what some regulations already require (e.g., the

Payment Card Industry's Data Security Standard) and is the direction other regulations are heading. If you deploy an exit point security methodology, you cannot set your objects to be "deny by default."

3) **IBM recommends object level security.** IBM is pushing a couple of things when it comes to security. They are pushing the idea of policy-based security and implementing object level security. They have NO commercial Exit Point product and do not recommend Exit Points as a way to accomplish a secured environment.

4) **The biggest issue that Exit Point vendors have zeroed in on is the "difficulty" of deploying an object level security scheme.** Their claim is that it is much easier to deploy, manage and maintain an exit point scheme. Early on, they might have had a point, however, one needs to take into consideration the fact that as an exit point environment gets more complex (that is, you have to manage more than just a couple of ways people might access data – SQL, ODBC, DDM, ETC) that allowing for such considerations yields an "exit point access granting" mechanism that is more functionally complex than object level security. The argument that exit points are easy to deploy, manage and maintain quickly goes out the window. Object level security may have been difficult to implement early on, however, with the advent of SkyView Policy Minder, deploying an object level security architecture is much quicker and easier and provides a total solution to controlling access to confidential, sensitive and private data.

Bottom-line is this: Object Level Security is the best method of controlling access to objects because it provides a complete solution. Regardless of how an object is accessed, i5/OS object level security (not an exit point vendors' so-called object level security) is in effect.

i5/OS object level security satisfies the regulations that require implementation of "deny by default" and it is inherent in (that is, tightly integrated into) the i5/OS operating system. Finally, i5/OS object level security does not cause any of the performance problems that can be inherent with the implementation of exit point programs.

***Carol Woodbury** is co-founder of SkyView Partners, Inc., a firm specializing in security policy compliance and assessment software as well as security services. Carol is the former Chief Security Architect for AS/400 for IBM in Rochester, Minnesota, and has specialized in security architecture, design, and consulting for more than 17 years. Carol is an award-winning speaker and writer and is coauthor of the book Experts' Guide to OS/400 and i5/OS Security.*