WHAT IS YOUR SECURITY EXPOSURE?

With PATHFINDER's Security Menu (HAWKSEC), it is possible to do a full-blown security audit. But, there are also a couple of summary reports which allow you to quickly get an idea of the potential security exposures on your iSeries (AS/400, Power System, System i). This article will focus on one of these summary reports, option "2. Security Checkup".

The Security Checkup Report compares your system to recommendations based on IBM's Security Reference Manual, the IBM security red book, and professional iSeries security auditors. The security checks which do not meet the recommendations will print on the report. Each security check has a rating assigned. The rating is a gauge of your system's potential security exposure. The higher the number, the greater the security risk.

Recommended steps to eliminate the exposure are listed. In some cases, another security option is suggested to provide additional detail.

Security checks and potential risk

Each security system value will be compared to recommended values. The Security Checkup report gives a summarized total rating. For detail on individual security system values, the "Security System Values Report" is provided (option 3 on the Security Menu).

Many checks are performed on user profiles. A message will print:

- When profiles have not been used in the last 60 days. This helps you keep the system clean of user profiles which are no longer being used.
- When the profile's password has not been changed in the last 90 days. Requiring users to change their passwords after a specified length of time reduces the risk of unauthorized access to your system.
- If a value other than *SYSVAL is specified for the parameters PWDEXPITV (Password Expiration Interval), LMTDEVSSN (Limit Device Session) or DSPSGNINF (Display Sign-on Information). This helps you control users with special values for these parameters and better ensures that an intended global change to one of these security system values would be incorporated into all user profiles.
- If the authority to the user profile is not *PUBLIC (EXCLUDE). This prevents unauthorized changes to the user profile.
- If the special authorities *ALLOBJ, *SERVICE, or *SPLCTL have been assigned. Giving special authorities to users represents a security exposure. For each user, carefully evaluate the need for any special authority.
- If an INLPGM (Initial Program) is specified and *SIGNOFF has not been specified for INLMNU (Initial Menu). An initial program is generally specified to limit the access of the user. If the default for INLMNU is not changed to *SIGNOFF, the user may have access to

more than was intended. Either an initial program or an initial menu should be used, but not both.

For those profiles which are user class *USER, a message will print:

- If *NO is specified for LMTCPB (Limit Capabilities). This controls which options would be available on the IBM Menus, as well as the ability to enter commands on the command line.
- If *SIGNOFF is not specified for INLMNU (Initial Menu). Many *USER profiles do not need access to the IBM Menus. Generally, *USER profiles are controlled with an initial program for tighter security.

For group profiles, a message will print:

- If the group profile has a password. Group profiles should not be used to sign on; they are intended as an administrative convenience to group users with similar requirements. Accountability is better maintained when only individual users are able to sign on.
- If the special authorities *ALLOBJ, *AUDIT, *SECADM, *SERVICE or *SPLCTL have been assigned. Giving special authorities to users represents a security exposure. For each user, carefully evaluate the need for any special authority.

A message will also print under the following conditions:

- A job description has a user profile and the authority to that job description is not *PUBLIC(*EXCLUDE). If a user is allowed to use a job description with a user profile specified, they will be running under that user profile's authority, not their own. This could give the user additional authority.
- A workstation entry of a subsystem description has a job description with a user profile specified. This could allow sign-on by just pressing the Enter key from the sign-on screen.
- Programs which adopt their owner's authority do not have *PUBLIC (*EXCLUDE) authority. If a user is allowed to run an adopting program, they will be running under the authority of the program's owner, not their own. This could give the user additional authority.
- The message queue QSYSMSG exists, but has not been cleared recently. If this message queue has been created on your system, security related messages will be sent to it. If this message queue has not been cleared, perhaps these security messages are not being monitored.
- Systems libraries do not have *PUBLIC (*USE) authority. *USE authority prevents users from replacing objects in these libraries with their own and ensures that the integrity of the system libraries remains intact.
- IBM-supplied profiles do not have *NONE for their password. These profiles should not be used to sign on.
- The security audit journal exists but authority to it is not *PUBLIC (*EXCLUDE), or the journal has not been changed in the last 30 days. Since all security related events are

logged here, it is good practice to limit access and prevent tampering. If the journal is not changed on a regular basis, it may indicate that it is not being properly monitored.

- Libraries appear higher than QSYS in the system value QSYSLIBL. This could allow a user-written command to execute in place of an IBM command.
- A library, with authority not *PUBLIC (*USE), appears higher than QSYS in the system portion of the library list. *USE authority prevents users from replacing objects in these libraries with their own. Since system libraries are searched first, if a user's object were used instead of a system object, this could circumvent security.
- A command in QSYS and its corresponding command in QSYS38 have different authorities. This helps you ensure any special authority changes to the commands in QSYS are also incorporated into QSYS38.
- The value for JOBACN (Job Action) in the network attributes is *SEARCH. *REJECT should be used if remote job requests are not expected, otherwise *FILE causes any incoming input streams to be filed on the queue of the network files for the receiving user.
- The system data (SAVSYS), configuration data (SAVCFG), or security data (SAVSECDTA) has not been saved in the last 30 days. This helps you ensure that this data is available to restore in case of a system failure.

A complete list of security checks can be found in PATHFINDER's Reference Manual, or in the help text printed on the Security Checkup Report (see "F18=Change defaults").

The package is shipped with the ratings set for a high security environment. Each security check is a message in the H$SECURITY message file. The message severity determines the rating. You can change these ratings to better fit your system's security requirements by changing the message severity. When the Security Checkup Report is submitted, the "Source of ratings" parameter determines which ratings will be used, "*PKG" (PATHFINDER's shipped ratings) or "*USER" (ratings customized to your environment).

To further discuss this insightful option, please contact our Technical Services department. We can be reached by email at info.hawkinfo.com or call us Monday-Thursday, 7 a.m. to 5 p.m. (MST) and Friday 7 a.m. to 3 p.m., VOICE (970) 498-9000 or FAX (970) 498-9096.